AV-Comparatives



Mobile Security Review

Sprache: Deutsch

August 2015
Letzte Überarbeitung: 17. September 2015

www.av-comparatives.org

Inhalt

Einleitung

Smartphones stellen die Zukunft der modernen Kommunikation dar. Laut einer Erhebung vom März 2015 sind alleine auf der Android Plattform über 1,6 Milliarden Smartphones im Umlauf[1]. Klassische Funktionen eines Telefons treten immer mehr in den Hintergrund. Durch die guten Kameras muss das Smartphone immer häufiger als Fotoapparat dienen. Neben den Fotos vertrauen die Benutzer durch Dienste wie Facebook, WhatsApp und Email ihrem Smartphone praktisch ihr ganzes Leben an. Dies bringt einige Risiken mit sich, denn mit diesen Eigenschaften wird das Smartphone auch für Kriminelle interessant, die versuchen, das Handy zu infizieren oder sensible Daten auszuspionieren. Gefährlich sind auch Attacken auf persönliche Daten oder Phishing-Angriffe.

Der Einsatz eines PCs oder Laptops ohne Security-Software ist inzwischen undenkbar. Bei Mobiltelefonen ist dieses Verantwortungsbewusstsein bei vielen der Nutzer leider noch nicht angekommen. Dabei enthalten sie oft wichtige persönliche Daten, private Fotos, Internetbanking Informationen oder sogar Firmendaten.

Da moderne Smartphones oft teuer sind, werden sie zudem immer öfters das Ziel von Dieben. Hochpreisige Smartphones lassen sich durchaus für mehrere hundert Euro verkaufen. Da Diebstähle an sich nicht zu verhindern sind, muss der Anreiz eines Diebstahles wegfallen. Deshalb verfügen viele der aktuellen Sicherheitsprodukte neben dem klassischen Antivirenschutz über ausgereifte Diebstahlschutzfunktionen, welche einen Diebstahl für Diebe weniger attraktiv machen – wie etwa dem Sperren des Geräts, oder beim Wiederfinden des Geräts helfen sollen.

Auch in diesem Jahr haben wir Sicherheitsprodukte für Mobiltelefone unter Google Android getestet. In unserem Bericht finden Sie Details zu den Produkten führender Anbieter, die sich bereit erklärt haben ihr Produkt unserer Überprüfung zu stellen. Der Test wurde im Juli und August 2015 unter Android 5.1.1 auf einem LG Nexus 5 durchgeführt.

Allgemein konnten wir feststellen, dass es unter der aktuellen Android Version durchwegs Probleme beim Blockieren von SMS gibt. Kein Sicherheitsprodukt konnte damit umgehen. Von vielen Herstellern wird dies auch entsprechend so kommuniziert. SMS können unter Android 5.1 nicht unterdrückt oder unsichtbar gemacht werden. Problematisch wird dieser Zustand vor allem bei Produkten, die bei der Diebstahlsicherung auf SMS Kommandos setzen. Dieben ist es daher möglich SMS in Klartext zu lesen und das Passwort einzusehen. Wir empfehlen den Herstellern ein Passwort für den Lockscreen zu vergeben das sich von jenem der SMS Kommandos unterscheidet. In Produkten wo dies bereits implementiert wurde empfehlen wir dem Nutzer zuerst einen Lockbefehl abzuschicken, um zu verhindern, dass Diebe Nachrichten in Hangouts lesen können. Dies ist der einzige Weg um Diebe vom Lesen der SMS abzuhalten.

Securitysoftware für Android erfordert in der Regel eine sehr große Anzahl an Berechtigungen, welche sie auf dem Smartphone erteilt bekommen. Zwischen den einzelnen Produkten konnten wir teilweise große Unterschiede ausmachen. Wir haben uns dazu entschlossen auch im diesjährigen Bericht eine Tabelle mit allen Berechtigungen zu veröffentlichen, welche im Appendix auf Seite 72 nachgelesen werden kann.

[1] http://de.statista.com/statistik/daten/studie/246004/umfrage/weltweiter-bestand-an-smartphones-nach-betriebssystem/



Diebstahlschutz

Der Diebstahlschutz gehört neben dem Malwareschutz zu den wichtigsten Komponenten einer mobilen Sicherheitsapp für Android. Es ermöglicht dem Nutzer auf seinem gestohlenen oder verlorenen Gerät bestimme Aktionen aus der Ferne auszuführen. Diese dienen in erster Linie dem Schutz der Privatsphäre und dem Wiedererlangen des Geräts. Der Remotezugriff erfolgt hierbei über ein Webinterface oder per SMS. Ersteres bietet den Vorteil, dass der Nutzer interaktiv durch den Vorgang geleitet wird, SMS-Befehle hingegen bieten den Vorteil, dass sie verlässlicher am Gerät ankommen. Dies gilt insbesondere für Aufenthalte im Ausland, bei deaktiviertem Datenroaming. Reicht es beim Remotezugriff über das Webinterface aus, die nötigen Login Daten zu kenn, müssen beim Zugriff über SMS die herstellerspezifischen Befehle bekannt sein. Hierfür wird stets ein Kennwort benötigt, welches im Vorfeld definiert werden kann. Manche Hersteller erlauben hierbei nur SMS-Befehle von vordefinierten Nummern.

Die Kernfunktionen eines Diebstahlschutzes dienen vor allem dem Schutz der persönlichen Daten. Selbst wenn das Gerät gestohlen werden sollte dürfen Dritte keinesfalls Zugang zu vertraulichen Daten wie Emails erhalten. Als erster Schritt wird in der Regel eine Sperrung des Geräts eingeleitet. Dies ist vergleichbar mit dem Sperrbildschirm von Android. Erst nach korrekter Eingabe des PINs oder Passworts kann das Gerät weiter verwendet werden. Als nächstes kann das Gerät geortet werden. Die meisten Hersteller zeigen die Position des Geräts auf einer Onlinekarte gängiger Anbieter an. Hilfreich kann bei der Suche nach einem verlegten Gerät auch die Alarm-Funktion sein. Sie lässt eine Melodie ertönen, die bei der Suche in den eigenen vier Wänden hilfreich sein kann. Ist für die Deaktivierung des Alarms ein PIN oder Passwort notwendig, so kann es auch für einen Dieb ein Anreiz sein das Gerät so schnell wie möglich wieder loszuwerden um keine Aufmerksamkeit auf sich zu lenken. Wenn auf ein Wiederlangen des Geräts nicht mehr zu hoffen ist können im finalen Schritt sämtliche persönliche Daten vom Gerät gelöscht werden.

Lock

Die Lock Funktion sperrt das Gerät des Eigentümers und soll vor Zugriff Unbefugter schützen. Ein Sperrbildschirm darf keinesfalls einfach umgangen werden können. Einige Hersteller verwenden als PIN für den Sperrbildschirm das Kennwort des SMS Kommandos. Dies kann vor allem dann Problematisch sein, wenn der Nutzer SMS Benachrichtigungen auf dem Sperrbildschirm anzeigen lässt (Standardeinstellung in Android). Ein Dieb kann so leicht das Kennwort in Erfahrung bringen und das Gerät entsperren. Hersteller die auf derartige Mechanismen setzen sollten dringend Alternativen entwickeln und anbieten. Ein weiteres Problem, das bei einigen Produkten festzustellen war ist die Möglichkeit die Notification Leiste zu öffnen. Sie ermöglicht nicht nur den Flugzeugmodus zu aktivieren und so den Diebstahlschutz via Webinterface komplett lahmzulegen, sondern auch zu einem Gastkonto zu wechseln. Auch wenn Funktionen wie Telefonieren in diesem Modus standardmäßig deaktiviert sind ist es einem Unbefugten möglich das Gerät in eingeschränktem Umfang zu nutzen. Dass dieser Modus keinesfalls für Unbefugte zur Verfügung gestellt werden darf zeigt auch die Empfehlung seitens Google[2], welche besagt, das Gerät auch im Gastmodus nur vertrauenswürdigen Personen auszuhändigen. In unsere Bewertungskriterien ist auch die Möglichkeit eines benutzerdefinierten Sperrbildschirms eingeflossen. Solche Sperrbildschirme ermöglichen es zum Beispiel Kontaktdaten eines Notfallkontakts anzugeben, welche auch im Falle einer Sperrung angezeigt werden. Dies kann es etwa einem ehrlichen Finder ermöglichen einen Übergabetermin zu vereinbaren. Zudem ist es in unseren Augen wichtig, dass zu jedem Zeitpunkt die Möglichkeit besteht einen Notruf



[2] https://support.google.com/nexus/answer/2865944?hl=en



abzusetzen. Wenige Produkte bieten die Möglichkeit während der Sperre Fotos mit der Frontkamera aufzunehmen. Die es ermöglicht einen Dieb zu fotografieren und möglicherweise zu identifizieren.

In unseren Tests mussten wir feststellen, dass nicht alle Funktionen zur vollsten Zufriedenheit implementiert wurden. In einigen Fällen konnte der Sperrbildschirm durch Auslesen der SMS Benachrichtigungen deaktiviert werden. Andere Produkte ließen ein Öffnen der Notification Leiste zu, was das Wechseln zu einem Gastkonto ermöglichte. Auch auf die Möglichkeit eines Notrufs wurde bei einigen Apps vergessen. Lob muss man den Herstellern hingegen bei etwaigen Neustarts des Geräts aussprechen. Jeder hat das Smartphone nach einem Neustart sofort wieder gesperrt.

Sicherheitsapps können bei nicht gerooteten Geräten nicht verhindern, dass die Werkseinstellungen wiederhergestellt werden, etwa durch einen Hard-Reset. Auch wenn Sicherheitsmechanismen wie ein Lockscreen oder die SIM Protection noch so gut umgesetzt sind, kann nicht verhindert werden, dass ein Dieb über den Umweg eines Resets das Gerät ungestört für seine Zwecke verwenden kann. Somit ist der Fokus des Diebstahlschutzes mehr dem Schutz der persönlichen Daten als dem Schutz des Geräts an sich zuzuordnen.

Locate

Die Locate Funktion ermöglicht das Orten des Geräts wenn es verloren oder gestohlen wurde. Sinnvoll kann dies zum Beispiel sein, wenn sich der Eigentümer des Geräts nicht mehr erinnern kann wo er sein Smartphone liegengelassen hat. Einige Hersteller von mobiler Sicherheitssoftware raten jedoch explizit davon ab selbst auf Verbrecherjagd zu gehen und empfehlen stattdessen Kontakt zur Polizei aufzunehmen.
Locate Funktionen unterschiedlicher Hersteller unterscheiden sich meist nur geringfügig. Alle bieten das einmalige Orten des Geräts. Manche ermöglichen zusätzlich eine kontinuierliche Ortung in festen Zeitabständen, also das Aufzeichnen eines Bewegungsprofils. Die meisten Anbieter setzen auf Onlinekarten wo nach erfolgreicher Ortung die Position entsprechend eingetragen wird. Wenige versenden per SMS blanke Koordinaten und erwarten vom Nutzer, dass dieser diese manuell in bei einem Kartendienst seiner Wahl einträgt – ein wenig unhandlich, wie wir finden.

Wipe

Die Wipe Funktion löscht persönliche Daten vom Smartphone des Besitzers. Hierbei gibt es zwei unterschiedliche Versionen. Manche Hersteller setzen das Gerät auf Werkseinstellungen zurück was automatisch ein Löschen aller Daten nach sich zieht. Diese Methode hat den Nachteil, dass anschließend der Diebstahlschutz wie etwa Funktionen zum Orten nicht mehr aktiv sind. In diesem Fall sollte der Nutzer nicht mehr auf ein Wiedererlangen des Geräts hoffen. Andere Versionen des Wipes verzichten auf das Zurücksetzen auf Werkseinstellungen. Dies bietet den Vorteil, dass das Security App auf dem Gerät installiert und aktiv bleibt. Somit ist auch nach der Ausführung des Wipe Befehls der Diebstahlschutz nach wie vor aktiv. In einem derartigen Fall ist es wichtig, dass der Hersteller des Antivirenprodukts möglichst gründlich löscht und möglichst keine Daten vergisst. In unseren Tests konnte kein einziger Hersteller die SMS mit dieser Methode löschen, was auf Einschränkungen bei der verwendeten Androidversion und die hierfür verwendete App Hangouts zurückzuführen ist. Auch Browserverlauf und Favoriten wurden nicht bei allen getesteten Produkten gelöscht. Wir haben Wert darauf gelegt, dass die Verknüpfung des Googleaccounts mit dem Gerät aufgehoben wurde und ein Zugriff auf Mails, Kalender, Anrufverlauf und Kontakte verhindert wird. Außerdem ist wichtig, dass auch Dateien vom Speicher entfernt werden.



SIM Protection

Die SIM Protection speichert Metadaten zur SIM Karte des Nutzers. Dies ermöglicht später zu erkennen, wenn eine fremde SIM Karte, etwa die des Diebes, eingelegt wurde um das Gerät zu verwenden. In der Regel sperren die meisten Sicherheitsapps das Gerät sofort nach der Erkennung des Wechsels. Ein Zutun des Nutzers, etwa das Absetzen von SMS Kommandos, ist hierfür nicht notwendig. Manche Sicherheitsapps informieren eine vertrauenswürdige Person, welche im Vorfeld definiert werden muss, über den Wechsel der SIM Karte per SMS. So kann ein Nutzer den Dieb möglicherweise identifizieren oder telefonisch Kontakt aufnehmen.

Malwareschutz

Mit Hilfe des Malwareschutzes werden Mobiltelefone auf Schadsoftware durchsucht und diese entsprechend gelöscht oder in Quarantäne verschoben. Um diese Funktion effizient nutzen zu können, muss der Virenschutz mit Updates auf dem neuesten Stand gehalten werden. Aufpassen muss man im Ausland, damit man mit automatischen Updates und Cloud-Scannern nicht in die Roaming-Falle tappt. Die Resultate zur Anti-Malware-Schutzleistung sind auf Seite 13 aufgelistet.



Kurzübersicht

Das perfekte mobile Security-Produkt gibt es noch nicht. Hier gilt es, wie bei den Windows-Produkten, sich über die Vor- und Nachteile in unserem Report zu informieren und eine Vorauswahl zu treffen. Empfehlenswert ist die Installation kostenloser Testversionen der infrage kommenden Produkte, welche sich ein paar Tage lang ausprobieren lassen. Danach wird die Entscheidung leichter fallen. Gerade im Bereich der Android-Security-Produkte werden sehr schnell neue Versionen veröffentlicht, die Verbesserungen und neue Funktionen beinhalten.



Mit der Teilnahme am Test haben die Hersteller ihr Engagement bewiesen, gute mobile Sicherheitssoftware für ihre Kunden zur Verfügung zu stellen. Wie in diesem Report zu lesen ist, haben wir bei vielen Produkten noch Fehler oder Funktionen gefunden, die nicht einwandfrei arbeiten. Die betroffenen Hersteller nehmen diese Probleme sehr ernst und arbeiten bereits an Lösungen. Da die Kernfunktionen der Produkte bei allen Herstellern bereits einen sehr guten Standard aufweisen, freuen wir uns, allen getesteten Sicherheitssoftwareprodukten unseren „Approved Award" überreichen zu können. Wir konnten auch im diesjährigen Test signifikante Verbesserungen zu den Vorjahresversionen feststellen.

AhnLab V3 Mobile ist ein Sicherheitsprodukt für Android, das die wichtigsten Sicherheitsfunktionen für Smartphones bietet. Premiumfunktionen wie App-Sperre und URL Scan runden das Angebot ab.

Antiy AVL for Android bietet reinen Malwareschutz mit einer Vielzahl an Einstellmöglichkeiten. Zusätzlich wird eine Callblocking Funktion geboten.

Ein sehr umfangreiches Sicherheitsprodukt mit einer Vielzahl an Einstellmöglichkeiten erhält der Nutzer mit A**vast Mobile Security**. Über ‚Shields' wird der Nutzer vor unterschiedlichen Gefahren geschützt.

AVG AntiVirus ist ein umfangreiches Sicherheitsprodukt, welches neben Malware- und Diebstahlschutz zusätzlich über eine Performance- und Privacy Komponente.

Avira Antivirus Security ist ein sehr schickes Security-App für Android Smartphones und bietet alle wichtigen Funktionen. Der Diebstahlschutz wird über ein Webinterface gesteuert. Im Vergleich zur Vorjahresversion wurde das App um einige Funktionen erweitert.

Baidu Mobile Guard ist ein sehr einfach zu verwendendes Sicherheitsprodukt für Android Smartphones. Es bietet viele Funktionen, wie etwa Optimierungsfunktionen, App Manager und Anti Spam.

Bitdefender Mobile Security & Antivirus bietet neben der Malware- und Anti-Theft Komponente umfangreiche Funktionen wie den App-Lock und den Privacy Advisor.

Cheetah Mobile setzt mit der Software **Clean Master** auf die Bereinigung des Mobiltelefons. Neben einem Virenscanner werden auch andere Funktionen wie RAM- und Telefonspeicherbereinigung geboten.



Cheetah Mobile CM Security Antivirus ist ein solide implementiertes Sicherheitsprodukt für Android Smartphones, welches wichtige Funktionen wie Antivirus und Diebstahlschutz bietet.

ESET Mobile Security & Antivirus bietet ein durchdachtes und schön gestaltetes App für Android Smartphones. Die Funktionen wurden solide implementiert und konnten überzeugen.

G Data Internet Security bietet neben dem Standardrepertoire auch ausgefeilten Schutz für Kinder. So ist ein Kid's Browser, ein Children's corner und weitere Funktionen, welche hilfreich für den Schutz von Kindern sein können, inkludiert.

Der Funktionsumfang von **Kaspersky Internet Security** ist groß, so werden neben einem Virenscanner auch SMS & Call Filter, Browserschutz, Diebstahlschutz und mehr geboten.

McAfee bietet mit dem Sicherheitsprodukt **Security & Antivirus** ausgereifte Software, die neben gängigen Features auch innovative Funktionen, wie eine CaptureCam und eine Profilverwaltung bietet.

Sophos Antivirus & Security bietet viele sinnvolle Funktionen die aktiv zur Sicherheit des Nutzers beitragen. Erwähnenswert ist der Security Advisor, welcher auf mögliche kritische Einstellungen hinweist, sowie eine gut gestaltete Spam Protection Komponente.

Tencent Mobile Manager ist ein Sicherheitsprodukt für Android mit einem großen Funktionsumfang betreffend Malware- und Datenschutz. Die Bedienbarkeit wurde erneut verbessert.

Mobile Security & Antivirus von **Trend Micro** bietet neben den wichtigsten Schutzfunktionen wie dem Diebstahlschutz und Malwarescanner zusätzlich sinnvolle Erweiterungen wie sicheres Surfen und schön gestalteter Kindersicherung.



Getestete Produkte

Die unten angeführten Produkte wurden in diesem Report getestet. Die aktuellste Version der Produkte wurde aus führenden App Stores wie dem Google Play Store im Juli 2015 bezogen. Die Hersteller hatten nach dem Test die Gelegenheit gefundene Fehler zu beheben. Falls Sie diese Fehler behoben haben, wurde dies im Report entsprechend angemerkt.

- AhnLab V3 Mobile Security 3.0.3.4
- Antiy AVL for Android 2.3.12
- Avast Mobile Security & Antivirus 4.0.7886
- AVG AntiVirus 4.4
- Avira Antivirus Security 4.1
- Baidu Mobile Guard 6.6.0
- Bitdefender Mobile Security & Antivirus 3.0.135
- Cheetah Mobile Clean Master 2.6.8
- Cheetah Mobile CM Security Antivirus 5.10.3
- ESET Mobile Security & Antivirus 3.0.1318
- G Data Internet Security 25.8.3
- Kaspersky Internet Security 11.8.4.625
- McAfee Security & Antivirus 4.4.0.467
- Sophos Free Antivirus and Security 5.0.1515
- Tencent Mobile Manager 5.6.0
- Trend Micro Mobile Security & Antivirus 6.0



Die mobilen Produkte von **Baidu** und **Tencent** sind derzeit nur auf Chinesisch verfügbar.

Eine umfangreiche Übersicht der am Markt erhältlichen mobilen Produkte ist auf unserer Webseite auf http://www.av-comparatives.org/list-mobile/ verfügbar.



Batterieverbrauch

Den Batterieverbrauch eines Gerätes zu messen, scheint auf den ersten Blick sehr einfach zu sein. Geht man jedoch in die Tiefe, sieht man sehr schnell die Schwierigkeiten, die sich ergeben. Gerade bei Mobiltelefonen unterscheidet sich die Nutzung der einzelnen Anwender sehr stark. Manche legen starken Wert auf Multimedia, andere auf das Betrachten von Dokumenten, andere verwenden fast ausschließlich die Telefonfunktionen. Wir müssen hier zwischen Powerusern, die das Telefon wirklich in seinen ganzen technischen Eigenschaften ausreizen und Usern, die das Telefon nur als Mittel zum Zweck, sprich telefonieren, unterscheiden.

Für die Erstellung der Testprozedur, hat AV-Comparatives im April 2012 eine Umfrage durchgeführt, um die durchschnittliche Nutzung von Smartphones zu ermitteln. Über tausend Smartphone-Benutzer aus der ganzen Welt wurden anonym zum Thema Mobiltelefonnutzung befragt. Hier stellte sich heraus, dass die Smartphone-Nutzer die Möglichkeit ihres Telefons sehr gut ausnützen. 95% aller Smartphone Nutzer surfen und mailen mit ihrem Telefon, über 2/3 hören online Musik oder schauen sich Videos im Internet über ihr mobiles Endgerät an. Auffallend ist auch, dass 70% der User ihr Telefon nie abschalten.

Das Smartphone wird für die Anwender immer wichtiger, fast kein Benutzer lässt eine Funktion ungenutzt. Das Telefon als allgegenwärtiges Kommunikationsmittel rückt immer mehr als Ergänzung, teilweise schon als Computerersatz in den Mittelpunkt.

Die Telefonie rückt beim Smartphone eher in den Hintergrund, mehr als 41% der User verwenden ihr Telefon nur 1-10 Minuten am Tag für Gespräche. Die meisten sind länger im Internet - über 29% länger als eine Stunde am Tag.

Die Werte aus unserer Mobile Security Umfrage (April 2012) haben wir als Basis für unsere Messungen verwendet. Anhand der daraus gewonnenen Daten haben wir den Einfluss der Security Software auf den Batterieverbrauch der einzelnen Smartphones auf einen Durchschnittsverbrauch berechnet.

Basierend auf den Umfragedaten wurden für die Batterieverbrauchsmessung folgende Nutzungsszenarien erhoben:

- **Telefonie** (30 Minuten pro Tag)
- **Bilder betrachten** (82 Minuten pro Tag)
- **Surfen im Internet** mit Android Browser (45 Minuten pro Tag)
- **YouTube Video mit YouTube App abspielen** (17 Minuten pro Tag)
- **Lokal gespeicherte Videos abspielen** (13 Minuten pro Tag)
- **Empfangen und Senden von Mails** unter Verwendung des Google Mail Clients (2 Minuten pro Tag)
- **Öffnen von lokalen Dokumenten** (1 Minute pro Tag)



In unserem Test konnten wir feststellen, dass die meisten mobilen Sicherheitsprodukte nur einen geringen Einfluss auf die Batterielaufzeit haben.

Hersteller	Batterieverbrauch	Hersteller	Batterieverbrauch
AhnLab		Cheetah Mobile CM S.	
Antiy		ESET	
Avast		G Data	
AVG		Kaspersky Lab	
Avira		McAfee	
Baidu		Sophos	
Bitdefender		Tencent	
Cheetah Mobile C.M.		Trend Micro	

up to 3%
3 to 8%
8 to 15%
15 to 25%
more than 25%

Grundsätzlich dürfen wir den Herstellern der Security-Suites gute Noten ausstellen. Im diesjährigen Battery-Drain Test hat es jedoch ein Produkt gegeben, welchem wir einen erhöhten Batterieverbrauch nachweisen konnten: **McAfee**. Beim Surfen im Internet konnten wir einen erhöhten Batterieverbrauch feststellen. McAfee hat das Problem untersucht und bestätigt, dass ein erhöhter Batterieverbrauch zustandekommt, wenn mehere Tabs im Browser geöffnet sind.



Schutz vor Android-Schädlingen

Die Methoden der Angriffe auf das Mobiltelefon werden immer raffinierter. Mit betrügerischen Applikationen werden die Benutzer von Mobiltelefon gerne um Daten oder gar Geld betrogen. Damit ihnen das nicht so leicht passiert und Sie die Gefahr auf ein Minimum reduzieren, sollten sie u.a. folgende Punkt beachten: Laden Sie Apps nur von vertrauenswürdigen Quellen herunter wie z.B. Google-Play oder den Playstores des eigenen Anbieters. Vermeiden Sie die Playstores von Drittanbietern oder auch durch Sideloading[3]. Ein weiteres Indiz unseriöse Apps aufzudecken, sind z.B. die Rechte, die die App verlangt. Als Beispiel: eine Applikation, die die Geschwindigkeit per GPS misst (z.B. im Auto) benötigt keine Rechte um das Telefonbuch oder die Telefonprotokolle einzusehen. Selbstverständlich ist es nur ein Indiz und keine Bestätigung, dass diese Applikation bösartig sein könnte, aber es sollte Sie sensibilisieren und anregen, einen zweiten Blick darauf zu werfen. Auch die Bewertungen im App Store sind eine gute Richtlinie; vermeiden Sie Applikationen mit schlechten oder dubiosen Bewertungen. Ein gerootetes Telefon bietet Ihnen zwar mehr Möglichkeiten, aber gleichzeitig ist es für bösartige Applikationen leichter, die Kontrolle über ihr Smartphone zu übernehmen. Rechtlich ist es nicht klar, ob die Garantie für das Telefon noch aufrecht ist, wenn das Telefon gerootet wurde. In vielen Fällen wird die Garantie erlöschen.

Wie hoch ist die Gefahr sich am Android Mobiltelefon zu infizieren?

Diese Frage lässt sich schwer beantworten, sie hängt von vielen verschiedenen Faktoren ab. In westlichen Ländern, bei Benutzung der offiziellen Stores wie Google-Play ist das Risiko geringer, als in Asien. In Asien, insbesondere in China, gibt es sehr viele gerootete Telefone und viele inoffizielle Appstores. In den von Google nicht überwachten Appstores ist das Gefahrenpotenzial eine infizierte App zu erwischen höher, als in den offiziellen Appstores. Auch wird in Asien das Smartphone oft als Computerersatz verwendet sowie sehr stark im Online-Banking eingesetzt. Auch in Europa und den USA sind Online-Banking Apps im Vormarsch. In den westlichen Ländern ist das Risiko, wenn man sich an die offiziellen Stores mit ungerooteten Geräten hält, momentan noch relativ gering. Man muss aber auch ausdrücklich dazu sagen, dass „geringes Risiko“ nicht gleichzusetzen ist mit „kein Risiko“. Die Bedrohungslage kann sich schnell und dramatisch ändern. Für diesen Fall sollte man bereits gewappnet sein und eine Sicherheitssoftware auf dem Mobiltelefon installiert haben. Viel wichtiger und nützlicher als der Malwareschutz am Mobiletelefon ist aus unserer Sicht zurzeit der Schutz gegen den Datenverlust bei Verlust oder Diebstahl des Smartphones.

AVC UnDroid Analyser

An dieser Stelle dürfen wir auf unser neues System hinweisen, AVC UnDroid, welches Usern kostenlos zur Verfügung gestellt wird. Hierbei handelt es sich um ein statisches Analysetool zum Erkennen von verdächtiger Schadsoftware in Android Apps (APK Dateien) und bietet zudem umfangreiche Statistiken zu Android Malware und Adware. Nutzer können APK-Dateien hochladen und anschließend das Resultat verschiedenster Analysemechanismen einsehen.



Interessierte sind herzlich dazu eingeladen das System auf http://www.av-comparatives.org/avc-analyzer/ auszuprobieren.

[3] http://en.wikipedia.org/wiki/Sideloading



Test Set & Testergebnisse

Die eingesetzte Malware wurde von uns in den letzten Monaten vor Testbeginn gesammelt. Für die Erstellung eines repräsentativen Test Sets wurden 2365 bösartige Applikationen herangenommen. Sogenannte „potentiell unerwünschte Apps“ wurden nicht ins Test-Set aufgenommen.

Die Sicherheitsprodukte wurden am 13. Juli 2015 zuletzt aktualisiert und getestet. Der Test wurde mit aktiver Internetverbindung auf echten Android Smartphones durchgeführt (es wurden keine Emulatoren verwendet). Das Test Set bestand ausschließlich aus APK-Dateien. Nach einem On-Demand Scan wurde jede einzelne verbleibende Malware-App manuell installiert. Wir haben uns für diese Vorgehensweise entschlossen um Produkten die Möglichkeit zu bieten Malware mittels Echtzeitscanner zu erkennen.

Auch ein Fehlalarmtest wurde mit Apps aus dem Google Play Store und anderen App Stores durchgeführt. Wenn die Kategorisierung von Apps von (zumeist asiatische) Drittanbietern nach „clean apps never to be detected“ und „clean/grey apps which are OK to detect“ fragwürdig war wurden diese in unserem Test nicht verwendet (Bis jetzt gibt es noch keine Industriestandards zur Kategorisierung, obwohl z.B. AMTSO daran arbeitet). Wir zählten nur die False-Positives von Apps welche im Google Play Store verfügbar sind. Die Ergebnisse können nachfolgend eingesehen werden (sortiert nach Malwareerkennungsrate und Anzahl der False-Positives).

Mobile Protection Rates

	Protection Rate	False Positives
Trend Micro	100.0%	0
Bitdefender	100.0%	3
G Data	100.0%	3
Antiy	100.0%	5
CM Security	99.9%	0
CleanMaster	99.9%	0
ESET	99.9%	1
Tencent	99.9%	2
Ahnlab	99.9%	3
Avira	99.9%	3
Avast	99.9%	4
Kaspersky Lab	99.7%	0
McAfee	99.6%	2
Baidu	99.4%	0
Sophos	99.2%	0
AVG	98.4%	4

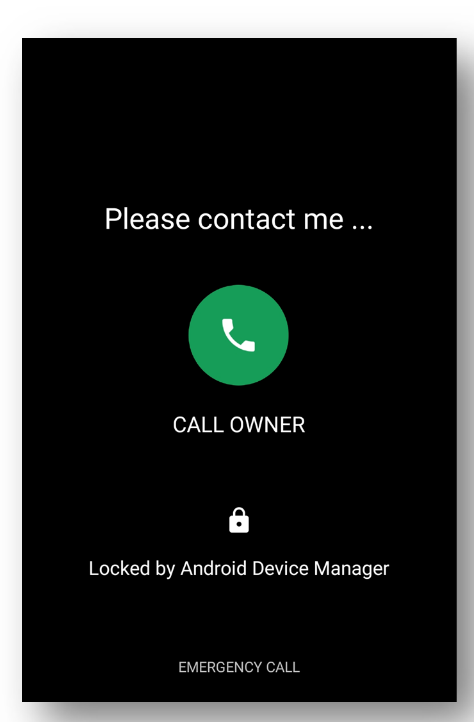


		Malware Schutz	Fehlalarme
1.	Trend Micro	100%	0
2.	Bitdefender, G Data	100%	3
3	Antiy	100%	5
4.	CM Security, CleanMaster	99,9%	0
5.	ESET	99,9%	1
6.	Tencent	99,9%	2
7.	AhnLab, Avira	99,9%	3
8.	Avast	99,9%	4
9.	Kaspersky Lab	99,7%	0
10.	McAfee	99,6%	2
11.	Baidu	99,4%	0
12.	Sophos	99,2%	0
13.	AVG	98,4%	4
14.	Android Baseline	unbekannt[4]	0

Wie in der Tabelle ersichtlich, ist der Schutz vor Android Malware sehr hoch. Dies könnte auf die steigende, aggressive Erkennung von Apps, welche nicht im Google Play Store aufscheinen, zurückzuführen sein, oder auch an der Tatsache, dass die Teilnehmer führende Experten im Gebiet der Malwareerkennung sind.

Android Security

Android Security der systemintegrierte Schutz welcher bereits am Gerät installiert ist und bietet Diebstahlschutz Funktionalität sowie die Möglichkeit Apps online zu verifizieren.



[4] Eine Erhebung der Erkennungsrate des Basisschutzes von Android konnte nicht durchgeführt werden da Google die Anzahl der Anfragen pro Gerät limitiert. Wir konnten keine Schutzraten für die Google Safebrowsing Service erheben. Anfragen an das Security Team von Google um unser Gerät zu whitelisten um solche Limitierungen aufzuheben wurden abermals nicht zeitgerecht beantwortet.

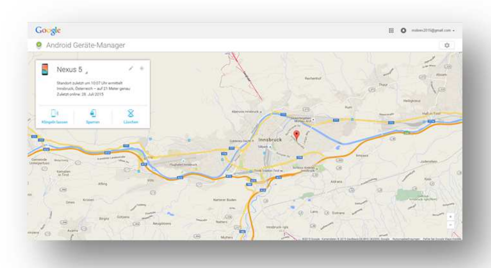


Installation

Die Installation des Schutzes entfällt, da sie bereits in Android integriert ist. Auf unserem Testgerät war die Funktion bereits standardmäßig aktiviert. Gegebenenfalls muss sie über „Google Settings > Security“ aktiviert werden.

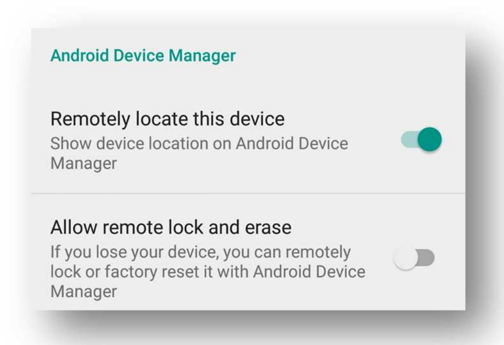
Diebstahlschutz

Android liefert einen Diebstahlschutz mit, welcher die wichtigsten Funktionen bietet. Die Steuerung dieser Komponente findet über ein Webinterface (https://www.google.com/android/devicemanager) statt. Hierfür ist ein Google Konto notwendig was aber bei der Verwendung von Android Geräten eigentlich immer der Fall ist. SMS Kommandos werden nicht angeboten.



Orten

Diese Funktion ortet ein gestohlenes oder verlorengegangenes Gerät und zeigt die Position auf einer Karte von Google Maps an. Dies findet jeweils automatisch nach dem Öffnen des Webinterfaces statt. Die Positionierung erfolgt jeweils nur einmalig – ein Aufzeichnen eines Bewegungsprofils wird nicht angeboten.



Klingeln Lassen

Die Klingeln Lassen Funktion lässt für fünf Minuten eine Melodie auf höchster Lautstärke ertönen. Hierbei handelt es sich um eine Funktion, welche zum Beispiel helfen kann ein verlegtes Handy innerhalb der eigenen vier Wände wiederzufinden. Das Gerät wird durch Absetzen des Kommandos nicht gesperrt. Durch Betätigen der Ein/Aus Taste kann das Klingeln gestoppt werden.

Sperren

Die Sperren-Funktion sperrt das Gerät mit dem Android Sperrbildschirm. So soll der Zugriff für Unbefugte unmöglich gemacht werden. Im Webinterface kann das Passwort für die Sperre direkt festgelegt werden. Gefallen hat uns, dass auf dem Sperrbildschirm eine Nachricht angezeigt werden kann, welche ebenfalls im Webinterface definierbar ist. Ein Anwendungsfall wäre etwa einem ehrlichen Finder Informationen zu geben wie er den Besitzer kontaktieren kann um das Gerät zurückzugeben. Zusätzlich kann eine Telefonnummer angegeben werden, die es Findern erlaubt direkt Kontakt mit dem Besitzer aufzunehmen. Über den Sperrbildschirm kann diese Nummer (nur diese) angerufen werden.



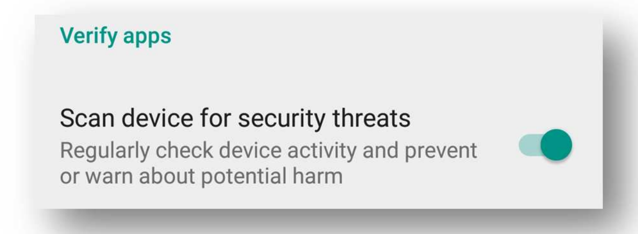
In unserem Test war die Sperrfunktion solide implementiert. Wir konnten sie nicht umgehen und hatten zu jedem Zeitpunkt die Möglichkeit einen Notruf abzusetzen. Einziges Manko: Es war möglich den Flugzeugmodus zu aktivieren. Danach war zum Beispiel die Ortungsfunktion nicht mehr aus der Ferne aktivierbar,

Löschen

Diese Funktion löscht die persönlichen Daten vom Smartphone des Nutzers. Nach dem Absetzen des Befehls wird das Gerät auf Werkseinstellungen zurückgesetzt.

Verify Apps

Android Security bietet dem Nutzer an installierte Apps regelmäßig zu überprüfen und gegebenenfalls vor schadhaften Apps zu warnen. Weitere Einstellmöglichkeiten als den Schutz zu aktivieren oder zu deaktivieren werden nicht angeboten. Wie bereits in der Einleitung erwähnt konnten wir die Erkennungsraten des Scanners aufgrund von Limitierungen nicht erheben.



Updates

Wir konnten keine Informationen bezüglich Updates von Virendefinitionen finden.

Hilfe

Es wird dem Nutzer kurze aber aussagekräftige Hilfe angeboten.

Deinstallation

Der Android Device Manager kann nicht deinstalliert, lediglich deaktiviert werden.

Lizenz

Der Schutz ist bereits vorinstalliert und kann kostenlos uneingeschränkt verwendet werden.

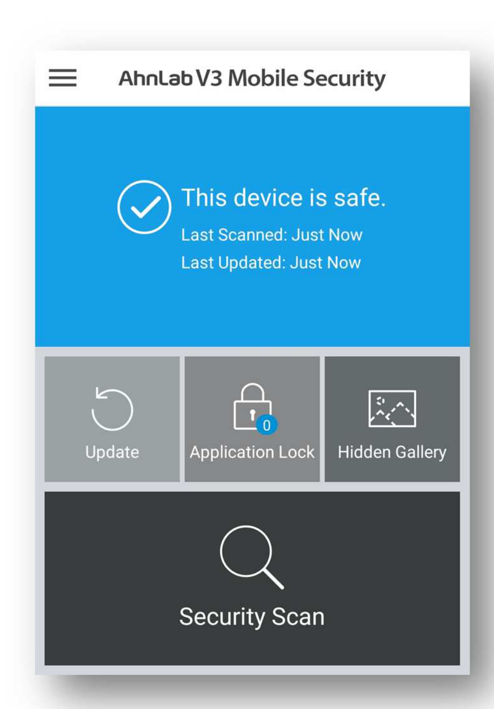
Fazit

Mit Android Security erhält der Nutzer die Basis Funktionalität an Diebstahl- und Malwareschutz. In unserem Test haben diese Funktionen einen stabilen und durchdachten Eindruck gemacht und können somit für so machen Nutzer als einfache Alternative zu einem externen Produkt überzeugen.



AhnLab V3 Mobile Security

Ahnlab V3 Mobile Security ist ein umfangreiches Sicherheitsprodukt das auch schon in der Free Version die wichtigsten Funktionen zur Verfügung stellt. Mit der Premium Version erhält man zusätzlich noch Funktionen wie App-Sperre und URL-Scan.



Installation

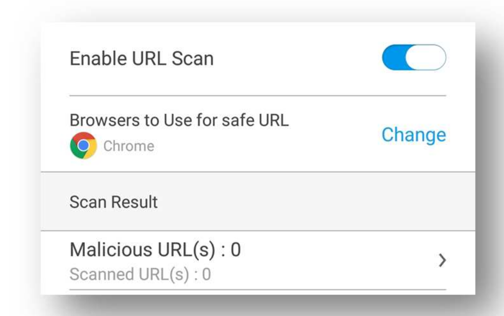
AhnLab V3 Mobile Security wurde aus dem Google Play Store bezogen und installiert. Nach dem Akzeptieren der EULA Lässt sich der Umfang von Malwarescans einstellen. Zusätzlich zu installierten Apps kann der Nutzer auch den Scann von Dateien veranlassen. Außerdem lässt sich in diesem Schritt die Erkennung von PUA aktivieren. Anschließend kann die Umgebung mit Updates definiert werden (Nur WiFi oder zusätzlich Mobilfunknetz). Anschließend wird ein Scan des Geräts gestartet und die Einrichtung ist abgeschlossen.

Malware Scan

Diese Funktion erlaubt die Überprüfung des Geräts auf Schadsoftware. Zusätzlich zur Echtzeiterkennung können Scans manuell angestoßen werden. Vor jeder Überprüfung wird erst die Virendatenbank aktualisiert.

URL Scan

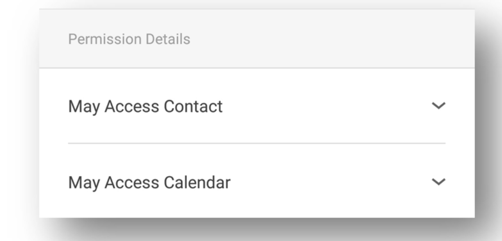
Der URL Scan schützt den Nutzer beim Surfen im Internet und muss vor der Nutzung aktiviert werden. In einem gut gestalteten Dialog wird der Nutzer durch die Konfiguration geleitet wo AhnLab als Standardprogramm für das Internetsurfen gewählt werden muss.



Gefallen hat uns, dass dennoch ein beliebiger Browser verwendet werden kann.

Privacy Advisor

Der Privacy Advisor macht den Nutzer auf Apps aufmerksam, welche viele Berechtigungen benötigen. Es werden vordefinierte Kategorien, wie zum Beispiel ‚Zugriff auf Kontakte', angezeigt. Dort werden Apps mit entsprechenden Berechtigungen gelistet.



Durch Tippen auf eines der Apps werden alle geforderten Berechtigungen aufgelistet.

Privacy Cleaner

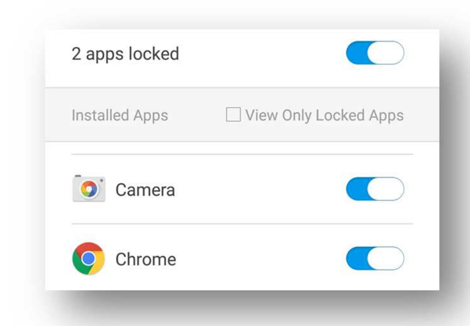
Der Privacy Cleaner löscht Dateien, die potenziell persönliche Daten enthalten. Es können Browser Logs sowie der Cache geleert werden.

Application Lock

Application Lock ermöglicht das Sperren von installierten Apps. Diese lassen sich dann erst nach Eingabe eines PINs starten. Dies kann



zum Beispiel sinnvoll sein wenn man das Gerät einem Kind überlassen und gewisse Apps von der Verwendung ausschließen möchte.

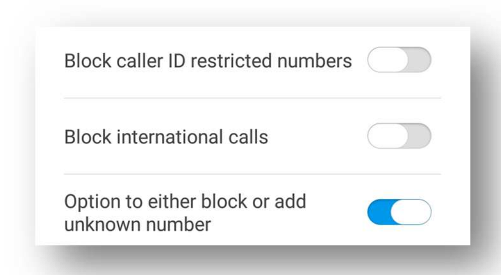


Hidden Gallery

Die Hidden Gallery versteckt ausgewählte Bilder und Videos auf dem Gerät. Diese werden in eine versteckte Galerie verschoben und sind dann nur noch nach Eingabe eines zuvor vergebenen PINs sichtbar.

Call Block

Die Call Block Komponente kann unerwünschte Anrufer abweisen. Hierfür werden Nummern zu einer Blacklist hinzugefügt. Gefallen hat uns, dass Nummern auch nach Mustern blockiert werden können. Dadurch lassen sich ganze Bereiche von Telefonnummern abdecken.



Außerdem lassen sich internationale- sowie unterdrückte Nummern grundsätzlich abweisen.

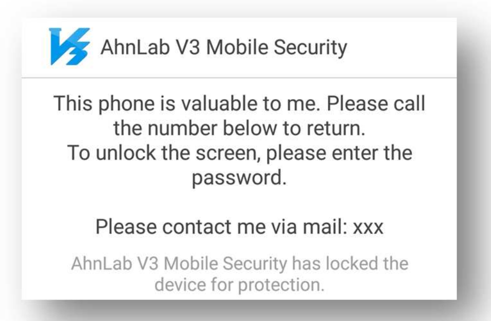
Anti-Theft

Auch für die Einrichtung des Diebstahlschutzes wird ein Wizard angeboten. AhnLab wird als Geräteadministrator registriert. Anschließend muss eine vertrauenswürdige Telefonnummer angegeben werden, welche im Falle eins SIM-Kartenwechsels verständigt wird. Im letzten Schritt kann eine personalisierte Nachricht für den Sperrbildschirm angegeben werden. Die Komponente wird über SMS Kommandos gesteuert. Ein Webinterface ist nicht verfügbar.

Lock Device

SMS Kommando: #lock <PIN>

Diese Funktion sperrt das Gerät mit dem PIN des SMS Kommandos. Hier hat AhnLab ziemlich gepatzt. In der getesteten Android Version werden SMS standardmäßig am Sperrbildschirm angezeigt, wodurch ein Dieb den PIN in Erfahrung bringen kann. Dramatisch wäre dies nicht, wenn man für den Sperrbildschirm einen anderen PIN oder ein Lock-Pattern vergeben könnte.



AhnLab überschreibt bestehende Sicherheitsfeatures jedoch einfach wodurch ein Zugriff auf das Gerät kinderleicht wird. Abhelfen kann sich ein Nutzer nur indem er in den Einstellungen sämtliche Notifications auf dem Sperrbildschirm deaktiviert. Auf diesen Zustand macht AhnLab jedoch nicht aufmerksam. Gefallen hat uns, dass nach der fünften falschen Eingabe des PINs ein Foto mit der Frontkamera aufgenommen wird. Dieses wird jedoch nur lokal auf dem Gerät gespeichert.

Track Location

SMS Kommando: #locate <PIN>

Dieses Kommando lokalisiert das Handy. Der Sender der SMS erhält als Antwort eine Nachricht mit den Koordinaten und einen Direktlink auf Google Maps. Die Antwort wird in zwei getrennten SMS versandt. Diese kann zu höheren Kosten führen, aus technischer Sicht wäre das nicht notwendig da beide Texte zusammen noch weit unter der maximalen Länge für SMS liegen.



Delete Data

SMS Kommando: #remove <PIN>

Dieses Kommando löscht persönliche Daten vom Gerät, jedoch nur dann wenn es von einer vertrauenswürdigen Nummer verschickt wird. Hierbei wird das Gerät nicht auf Werkseinstellungen zurückgesetzt. Hierfür muss das Kommando ***#wipe <PIN>*** gesendet werden. In unserem Test konnten wir kein Szenario provozieren indem die oben genannten Funktionen funktionierten. Als SMS-Antwort erhielten wir immer, dass das Kommando nicht von der vertrauenswürdigen Nummer gesendet wurde. (egal in welchem Format die Nummer angegeben wurde)

Send Alert

SMS Kommando: #ring <PIN>

Lässt für 20 Sekunden einen Alarm ertönen.

SIM Card Replacement

Es wird eine SMS an die eingetragenen vertrauenswürdige Nummer gesendet, welche über den Vorgang benachrichtigt. Die in der Hilfe Beschriebene Funktionalität *„Sets alert when SIM card is replaced.“* Ist hier etwas irreführend und sollte vielleicht auf „Send…“ geändert werden.

Updates

Die Virendefinition kann automatisch aktualisiert werden. Diese Funktion ist standardmäßig jedoch deaktiviert. Als Intervall kann täglich oder wöchentlich (+Wochentag) gewählt werden.

Hilfe

Zu jeder Komponente des Produkts existiert ein Abschnitt in einer Hilfedatei. Der Umfang ist kompakt und aussagekräftig.

Deinstallation

Für die Deinstallation wird kein Kennwort benötigt, es sei denn die Einstellungen sind mit Application Lock geschützt. Für die Deinstallation muss erst der Geräteadministrator deaktiviert werden.

Lizenz

Ahnlab V3 Mobile Security ist gratis aus dem Play Store installierbar und die ersten 10 Tage in der Premium Version gratis nutzbar. Es kann dann entweder die Free Version ohne, „Auto-block Malware“, „Hidden Galler“, „URL Scan“ und „Application Lock“ verwendet werden oder für €1,99 monatlich bzw. €14,44 jährlich die premium Version erworben werden.

Fazit

Das Produkt ist sehr einfach und angenehm zu bedienen, weist allerdings auch einige Probleme auf die auf die neue Android Version zurückzuführen sind. In unseren Tests hatten wir große Probleme mit der stabilen Funktionsweise der SMS-Kommandos und auch die Bildschirmsperre ließ sich durch die angezeigten SMS sehr einfach umgehen.



Antiy AVL for Android

AVL for Android konzentriert sich mit seinem geringen Funktionsumfang stark auf die Erkennung von Malware. Neben der Malware Erkennung wird lediglich eine Call Blocking Funktion angeboten.

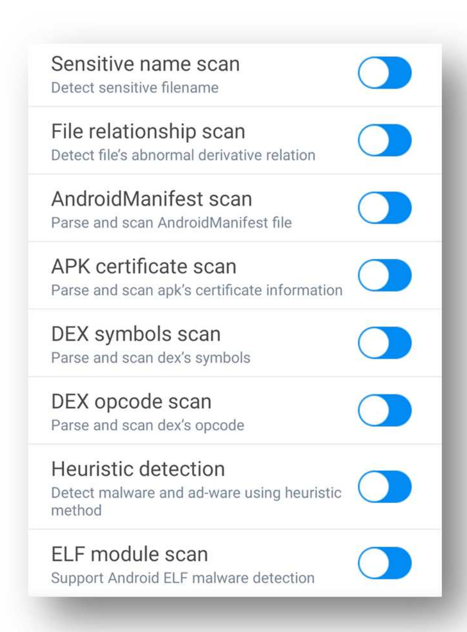


Installation

AVL for Android wurde aus dem Google Play Store bezogen und installiert. Die Installation erfordert keinerlei Zutun des Nutzers und ist in Sekundenschnelle erledigt.

App-Only Scan

Der App-Only Scan untersucht installierte Apps auf schadhaftes Verhalten. In den Einstellungen finden sich diverse Expertenoptionen um die Scans an persönliche Bedürfnisse anpassen zu können. So ist es möglich einzustellen ob der opcode der DEX Datei gescannt werden soll oder ob Heuristiken eingesetzt werden.



Custom Scan

Der Custom Scan erlaubt es den Speicher des Geräts auf Malware zu überprüfen. Mit Hilfe von Checkboxen werden die zu scannenden Ordner ausgewählt.

Safe Browsing

AVL bietet eine "Safe Browsing" Komponente, die den Nutzer vor schadhaften Webseiten schützt. Details zur Schutzfunktion konnten wir nicht finden. In unserem Kurztest mit Google Chrome konnten wir keine Erkennung provozieren.

Call Blocking

Um sich gegen unerwünschte Anrufer schützen zu können bietet AVL einen Call Blocker an. Dieser weist Anrufe, welcher auf der schwarzen Liste stehen ab. Nummern können über eine sehr schlicht gehaltene Maske hinzugefügt werden. Lästig ist, dass es nicht möglich ist Nummern aus Anruflogs oder Kontaktlisten zu importieren. Nummern müssen manuell hinzugefügt werden.

In unserem Test hat die Komponente nicht funktioniert. Obwohl wir versucht haben die zu blockierende Nummer mit unterschiedlichen Formaten der Vorwahl einzugeben haben wir keine Blockierung des Anrufs feststellen können.



Updates
Updates können täglich automatisch oder manuell durchgeführt werden.

Hilfe
Es gibt eine Hilfedatei, welche grundlegendes Wissen für mobiles Antivirus beinhaltet, etwa was Root-Berechtigungen sind. Zusätzlich werden implementierte Funktionen erläutert. Die Hilfe deckt jedoch nicht den gesamten Funktionsumfang des Sicherheitsprodukts ab. Wir konnten keine Funktionen zu Safe Browsing und Call Blocking finden.

Deinstallation
AVL for Android kann über den systeminternen App Manager deinstalliert werden.

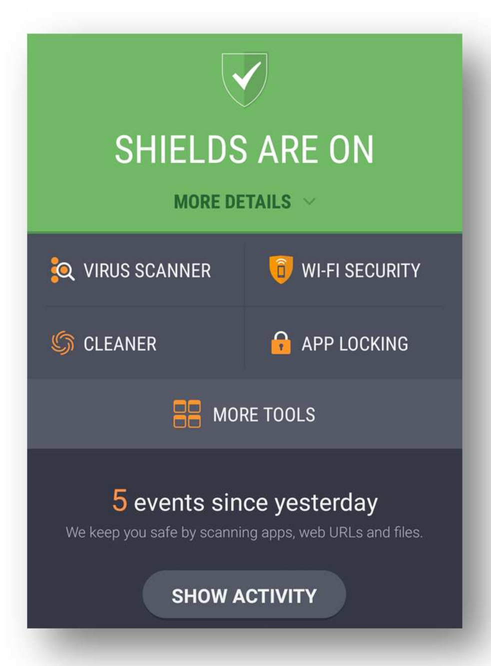
Lizenz
AVL for Android ist gratis im Google Play Store erhältlich.

Fazit
Man erkennt bei diesem Produkt sehr stark seinen Focus auf die Malwareerkennung. In unserem Test zählte die App in diesem Bereich mitunter zu den Besten. Wer allerdings noch andere Funktionen einer Sicherheitsapp, wie z.B. Anti-Theft nutzen möchte ist bei einem umfangreicheren Produkt besser aufgehoben. Im Gegensatz zum Malwareschutz funktionierten alle anderen Funktionen in unserem Test nur mangelhaft.



Avast Mobile Security

Avast Mobile Security ist eine gut durchdachte sehr umfangreiche Sicherheitsapp. Unter anderem bietet Avast auch Funktionen wie eine Firewall an, welche aber nur auf einem gerooteten Gerät verwendbar ist.

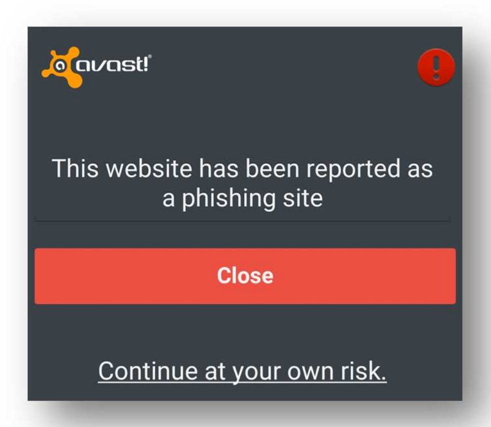


Installation

Avast Mobile Security wurde aus dem Google Play Store geladen und installiert. Nach dem Akzeptieren der EULA wird der Nutzer darauf hingewiesen, dass die *Shields* aktiviert wurden. Anschließend kann optional ein Scan der installierte Apps durchgeführt werden.

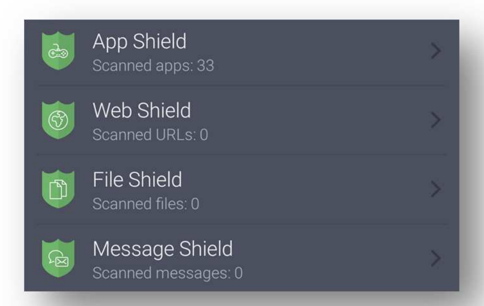
Shields

Verschiedenste Echtzeitschutzfunktionen werden bei Avast als *Shield* bezeichnet. Folgende Shields sind verfügbar: Das *App Shield* scannt je nach Einstellungen Apps während der Installation oder ihrer Ausführung.



Das *Web Shield* schützt den Nutzer während dem Surfen vor Phishingseiten oder jenen, die Schadcode enthalten. Hierbei wird sowohl der Standardbrowser, als auch Google Chrome, Amazon Silk und der Boat Browser unterstützt. Dies hat in unserem Kurztest auch gut funktioniert. Zusätzlich bietet avast! einen Spelling-Checker, der bei falsch getippten URLs eingreifen soll und diese richtig stellen soll. In unseren Tests haben wir jedoch keinen Fall produzieren können, wo Avast eingegriffen hätte. Avast hat uns darüber informiert, dass das Problem in der aktuellsten Version behoben wurde, welche aktuell verteilt wird.

Das Message Shield scannt alle eingehenden Nachrichten auf Phishing oder gefährliche URLs. Dies hat in unserem Test sauber funktioniert. Außerdem können Nachrichten mit unbekanntem Absender blockiert werden.



Das *File Shield* scannt Dateien während dem Lesen oder Schreiben auf schadhaftes Verhalten. Auch dies hat in unserem Test einwandfrei funktioniert.



Virus Scanner

Die Virus Scanner Komponente überprüft das Gerät auf Schadsoftware. Dabei kann der Nutzer den Scan von Apps und Dateien jeweils aktivieren oder deaktivieren. Gefallen hat uns, dass diese Komponente auch automatisiert, zeitgesteuert arbeiten kann. Über ein übersichtlich gestaltetes Menü können Scans in frei definierbaren Intervallen festgelegt werden.

Wi-Fi Security

Die Wi-Fi Security Komponente überprüft das aktuell verbundene Drahtlosnetzwerk auf Verwundbarkeit. Es wird auf schwache Verschlüsselung, ausnutzbare rom-0 Schwachstellen und schwache Routerpasswörter hingewiesen.

Cleaner

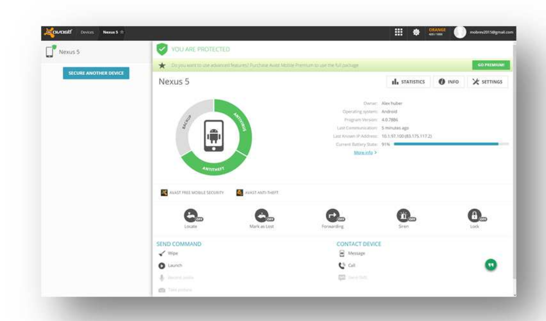
Die Cleaner Komponente ermöglicht das Bereinigen von Cache und Junk Dateien, ist jedoch nicht im Produkt integriert sondern wird lediglich direkt auf den Play Store verlinkt.

App Locking

App Locking ermöglicht das Sperren von installierten Apps. Diese lassen sich dann erst nach Eingabe eines PINs starten. Dies kann zum Beispiel sinnvoll sein wenn man das Gerät einem Kind überlassen und gewisse Apps von der Verwendung ausschließen möchte.

Anti Theft

Die Anti-Theft Komponente ist eine Stand-Alone Anwendung und muss nachträglich installiert werden. Dies bringt den Vorteil, dass die App versteckt werden kann.



Die Installation ist relativ schnell erledigt. Es muss lediglich der eigene Name und die Telefonnummer eines Freundes angegeben werden. Weil aktuelle Versionen von Android das versteckte Senden von SMS nicht mehr unterstützt, bietet Avast das Senden von binären Nachrichten, welche von Dieben zwar gelesen, aber nicht verstanden werden können. Durch die Aktivierung der Anti-Theft Komponente wird automatisch der Stealth Mode aktiviert, welcher die Diebstahlschutzfunktion komplett versteckt. Durch simples Anrufen des PINs wird die Komponente wieder sichtbar gemacht und angezeigt.

Der Diebstahlschutz wird über ein modernes Webinterface oder SMS Kommandos gesteuert. Neben den Klassikern wie Sperren, Lokalisieren und Löschen bietet Avast z.B. auch die Weiterleitung von SMS, Anruflisten, Umleitung von Anrufen, usw. Eine Übersicht aller Befehle findet sich hier: https://www.avast.com/free-mobile-security#premium (auf Button „Control via SMS“ klicken).

Locate

SMS Kommando: <PIN> LOCATE<INTERVALL>.

Mit diesem Kommando wird das Gerät geortet. Im Anschluss erhält der Sender eine Antwort-SMS mit einem Link auf eine Onlinekarte inklusive Koordinaten, Zellinformationen und Netzbetreiber. Durch den optionalen Parameter *Intervall*, das in Minuten angegeben wird, kann selbst über SMS ein kontinuierliches Tracken, ein Aufzeichnen des Bewegungsprofils, durchgeführt werden. Selbstverständlich hat der Nutzer auch die Möglichkeit diese Funktionalität über das Webinterface zu nutzen, wo der Bewegungsverlauf in einer Karte dargestellt wird. Diese Art der Darstellung eignet sich deutlich besser als das permanente Senden von SMS. Die kontinuierliche Ortung kann mit dem SMS Befehl „<PIN> LOCATE STOP“ angehalten werden.



Lock

SMS Kommando: <PIN> LOCK

Nach Absetzen des Kommandos wird das Gerät gesperrt und ein Lockscreen angezeigt. Ein ehrlicher Finder wird dazu aufgefordert eine Fundmeldung bei avast zu machen. Hierfür muss die IMEI, die während des Locks angezeigt wird, an android@avast.com gesendet werden. Dieser Anzeigetext kann jedoch editiert werden. Zusätzlich ertönt eine laute Sirene mit einem Ansagetext „*This phone has been lost or stolen*“. Diese ist nur in Englisch verfügbar. Durch Eingabe des richtigen PINs kann die Sperre aufgehoben werden.

Beim Sperrbildschirm war es möglich die Notification Leiste herunterzuziehen. So war es uns möglich zum Beispiel zu einem Gastkonto zu wechseln und das Gerät in diesem Modus zu verwenden. Außerdem kann so das Passwort des SMS Kommandos in den Benachrichtigungen einfach ausgelesen und die Bildschirmsperre umgangen werden. Avast ist sich dessen bewusst und warnt den Nutzer entsprechend. Abhilfe bietet das Senden von binären Nachrichten mit einem anderen Gerät mit Avast, sowie die Verwendung des Webinterfaces. Des Weiteren ist es nicht möglich bei gesperrtem Smartphone einen Notruf abzusetzen, was unter Umständen gefährlich werden kann.

Siren

SMS Kommando: <PIN> SIREN ON

Mit diesem Kommando wird derselbe Ton wie auch schon beim Sperren abgespielt, mit dem Unterschied, dass das Gerät nicht gesperrt wird. Diese Funktion dient somit nicht der Sicherheit, sondern dem Wiederfinden des Geräts, wenn es verlegt wurde.

Wipe

SMS Kommando: „<PIN> WIPE“

Diese Funktion löscht persönliche Daten vom Smartphone des Nutzers. Hierfür bietet avast! mehrere Optionen an. Bei der herkömmlichen Methode wird das Gerät nicht auf Werkseinstellungen zurückgesetzt. In unserem Test wurden persönliche Daten wie Kontakte, Lesezeichen und Kalendereinträge Dateien etc. gelöscht, jedoch nicht die SMS und der Google Account. Somit können Emails nach wie vor empfangen und gelesen werden.

Durch Setzen des Geräteadministrators in den Einstellungen hat Avast die Möglichkeit das Gerät bei einem Wipe auf Werkseinstellungen zurücksetzt. Bei diesem werden auch die SMS und der Google Account gelöscht, jedoch hat danach der Nutzer keine Möglichkeit mehr die Diebstahlschutzfunktionen zu verwenden. Zusätzlich bietet Avast noch die Option den SD-Karten Speicher zu überschreiben um ein Wiederherstellen er Daten zu erschweren.

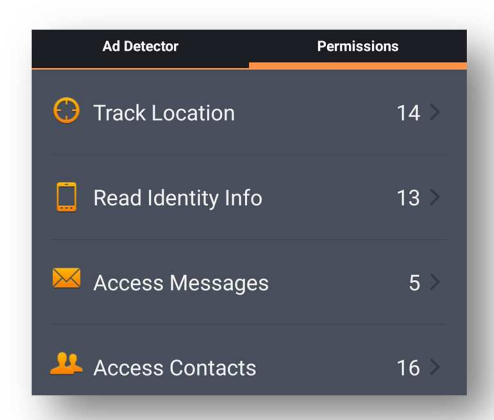
SIM Change Lock

Avast bietet eine Funktion an, welche das Gerät sperrt, wenn die SIM Karte getauscht wird, etwa wenn ein Dieb seine eigene einlegt. Der Nutzer kann einstellen welche Aktionen in einem derartigen Fall ausgeführt werden sollen, wie zum Beispiel das Sperren des Geräts und dem Abspielen eines Sirenensignals. Der Nutzer wird per Email über den Wechsel informiert, welche die Position des Geräts beinhaltet. Aus der Email geht allerdings nicht hervor, dass es sich bei der Aktion um ein SIM-Change Ereignis handelt.

Privacy Advisor

Der Privacy Advisor analysiert installierte Apps auf mögliche Datenschutzverletzungen. Apps werden in unterschiedliche Kategorien eingeteilt, wenn sie etwa Zugriff das Adressbuch oder die Nachrichten haben. Gefallen hat uns, dass zu jeder Berechtigung eine kurze Beschreibung mit möglichen Angriffsszenarien gegeben wird. Ähnliche Funktionalität bietet auch die Komponente *App Management*, welche zu allen laufenden und installierten Applikationen hilfreiche Informationen wie Speicher- und Prozessorauslastung bietet.





Zusätzlich zu den Berechtigungen bietet Avast einen Ad-Detector, welcher alle Werbenetzwerke, die in Apps integriert sind, anzeigt. So wird zum Beispiel Google Analytics, oder Mixpanel angezeigt. Zudem werden die Berechtigungen der Werbenetzwerke aufgelistet. Ein Beispiel wäre, ob es die Möglichkeit hat Netzwerkinformationen abzufragen oder das Nutzerverhalten aufzuzeichnen.

SMS & Call Filter

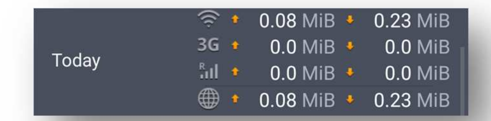
Um nicht von ungewünschten Anrufen bzw. SMS Nachrichten gestört zu werden, bietet avast! den *SMS & Call Filter* an. Hierfür können Gruppen angelegt werden, um Anrufe und SMS Nachrichten zu gewissen Zeitpunkten von bestimmten Mitgliedern zu blockieren.
Die Mitglieder können Kontakte aus dem Adressbuch, Rufnummern, alle anonymen Anrufer und unbekannten Teilnehmern sein. Es ist möglich mit Wildcards Einträge in der Blacklist zu erstellen um z.B. Nummern mit einer gewissen Vorwahl zu blocken. Avast verfolgt bei dieser Komponente den Ansatz des Blacklistings. Es werden also alle Anrufer durchgelassen, welche nicht explizit einer Gruppe zugeordnet sind.
Avast macht darauf aufmerksam, dass die Blockierung von SMS mit der Android Version nicht kompatibel ist.

Firewall

Wie auch schon im Vorjahr liefert Avast eine Firewall mit. Diese ist aufgrund der Sicherheitsbestimmungen von Android nur mit Root Zugriff verwendbar. Da für unsere Tests lediglich ungerootete Geräte verwendet werden, so wie sie bei den meisten Nutzern im Einsatz sind, haben wir diese Komponente nicht weiter getestet.

Network Meter

Diese Komponente listet den das verbrauchte Datenvolumen aller installierten Apps. Hierbei kann nach WiFi, 3G, Roaming und Gesamt aufgeschlüsselt werden. Durch Antippen einer der Apps wird das Transfervolumen zusätzlich nach Datum (Heute, Monat, Jahr) aufgeschlüsselt dargestellt.



Updates

Updates werden automatisch durchgeführt. Hierfür kann gewählt werden welche Netzwerke zur Verfügung stehen sollen (Wifi, 3G, Roaming). Zusätzlich können Updates auch manuell angestoßen werden.

Hilfe

In der App wird außer für die Anti Theft Komponente keine Hilfe angeboten. Auf der Webseite des Herstellers findet sich zwar ein Benutzerhandbuch, dieses ist jedoch offenbar veraltet. Neuere Funktionen, wie etwa die Wi-Fi Security Komponente, werden nicht erwähnt. Avast teilte uns mit, dass sie hier Verbesserungen planen.

Deinstallation

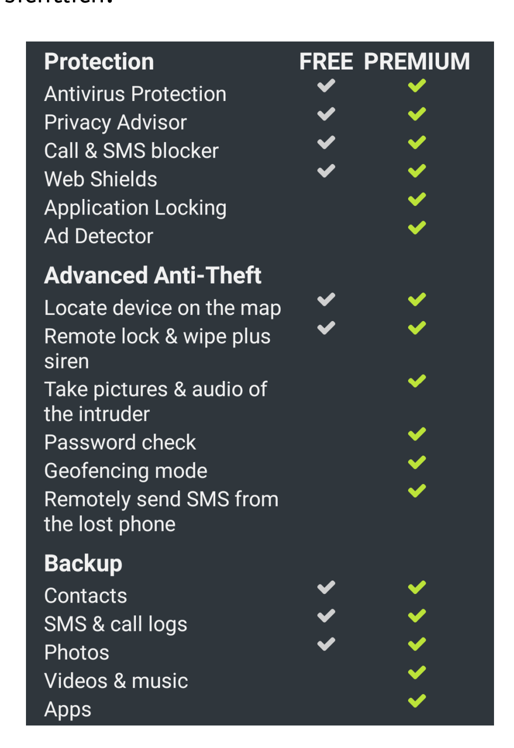
Die Deinstallation von avast! Mobile Security kann ohne Passworteingabe durchgeführt werden. Der Diebstahlschutz bleibt jedoch aktiv, da diese Komponente in eine separate App ausgelagert wurde.

Lizenz

Die gängigen Funktionen sind in der Free Version gratis verfügbar. Mit einem Upgrade auf die Premium Version erhält der Nutzer eine Vielzahl zusätzlicher nützlicher Funktionen.



Der volle Funktionsumfang ist im nächsten Bild ersichtlich.



Protection	FREE	PREMIUM
Antivirus Protection	✓	✓
Privacy Advisor	✓	✓
Call & SMS blocker	✓	✓
Web Shields	✓	✓
Application Locking		✓
Ad Detector		✓
Advanced Anti-Theft		
Locate device on the map	✓	✓
Remote lock & wipe plus siren	✓	✓
Take pictures & audio of the intruder		✓
Password check		✓
Geofencing mode		✓
Remotely send SMS from the lost phone		✓
Backup		
Contacts	✓	✓
SMS & call logs	✓	✓
Photos	✓	✓
Videos & music		✓
Apps		✓

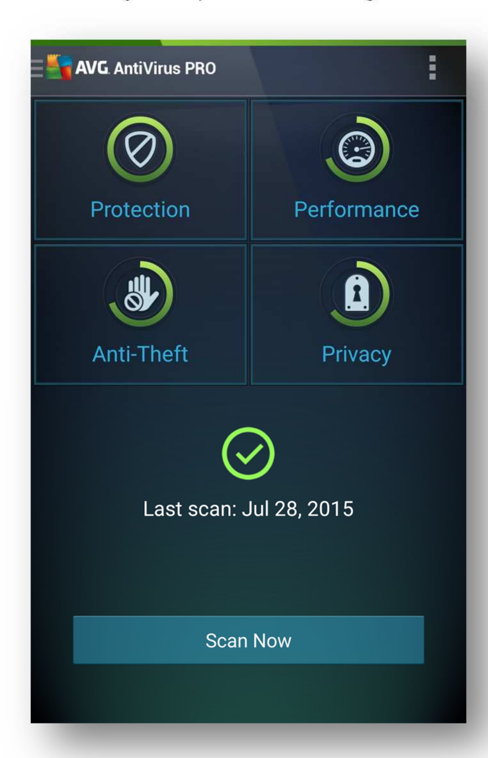
Fazit

Avast bietet wohl die App mit dem größten Funktionsumfang und bietet für Besitzer eines gerooteten Handys zusätlich Möglichkeiten es zu schützen. Die getesteten Funktionen funktionierten stabil, allerdings sind auch hier die für die neue Android Version typischen Probleme aufgetreten.



AVG AntiVirus

AVG AntiVirus ist ein umfangreiches Sicherheitsprodukt welches neben Malware und Diebstahlschutz auch über eine Performance und Privacy Komponente verfügt.



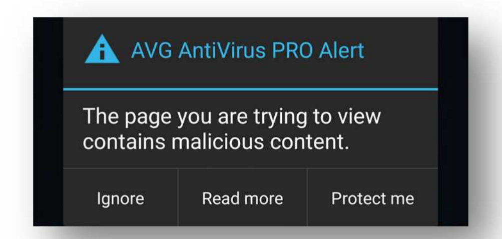
Installation

AVG AntiVirus Free wurde aus dem Google Play Store bezogen und installiert. Nach dem Akzeptieren der EULA kann sich der Nutzer entscheiden ob er die Gratis Version verwenden oder zur PRO Variante upgraden möchte.

Protection

Die Protection Komponente fasst Funktionen zusammen, welche den Schutz des Nutzers betreffen. Dazu gehört etwa ein Malwarescanner, welcher Schädlinge aufspüren und entfernen kann. Neben einem Systemscanner können über den Button „File Scanner" auch nur bestimmte Ordner auf dem Gerät untersucht werden. Außerdem ist es möglich die Sensitivität des Scanners einzustellen. Automatisierte Scans können sowohl täglich als auch wöchentlich ausgeführt werden. Gefallen hat uns, dass ein Systemscan nicht nur Schädlinge, sondern auch unsichere Einstellungen auf dem Gerät aufspüren kann. So wurde etwa kritisiert, dass auf unserem Testgerät USB Debugging aktiviert sei.

Versteckt in den Einstellungen findet sich zudem eine Checkbox, die das sichere Websurfen aktiviert oder deaktiviert. In unserem Kurztest hat die Komponente einwandfrei funktioniert und schädliche Webseiten gesperrt.



Performance

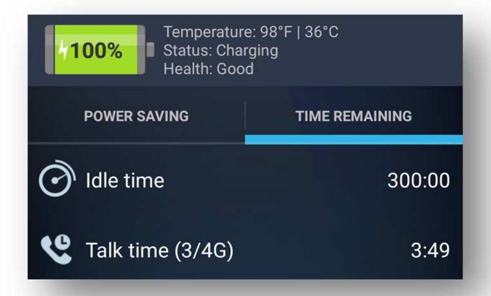
Unter dem Reiter Performance werden nachfolgende Komponenten betreffend Ressourcenbelastung zusammengefasst.

Task Killer

Der Task Killer ermöglicht das Beenden von einzelnen oder allen laufenden Apps. Über einen „Optimize" Button können alle laufenden Applikationen geschlossen werden.

Battery Consumption

Die Battery Consumption Komponente hilft die Batterielaufzeit des Geräts zu verlängern. Im Power Saving Mode können bestimmte Funktionen wie WiFi, Bluetooth, GPS und ähnliches deaktiviert werden. Zudem kann definiert werden ab welchem Akkustand dieser Modus aktiviert werden soll (10%, 30%, 50%).



In einer weiteren Ansicht wird basierend auf dem aktuellen Akkuladestand die verbleibende



Laufzeit für unterschiedliche Tätigkeiten, wie Telefonieren, Audio abspielen und Internetsurfen geschätzt.

Storage Usage

Die Storage Usage Komponente berechnet die Speichernutzung von installierten Apps und zeigt diese in einer Liste an. Durch einfaches Tippen auf das Müllkübelsymbol können die jeweiligen Applikationen deinstalliert werden.

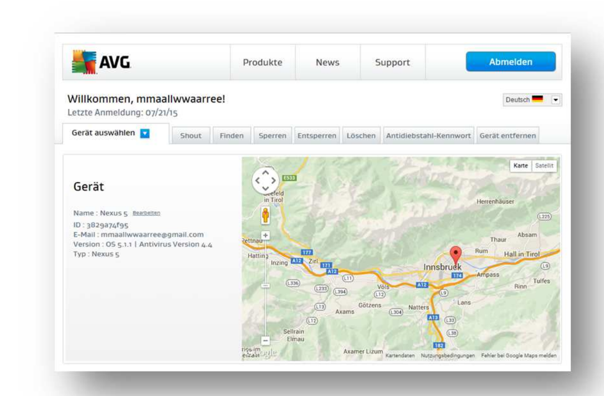
Data Plan

Data Plan überwacht das verbrauchte Datenvolumen für einen vorgegebenen Zeitraum. Der Nutzer kann einstellen wie viel Datenvolumen in seinem Vertrag zur Verfügung steht. Sollte er mit seiner Nutzung an die Grenzen dieses Limits gelangen, so kann er von AVG gewarnt werden.

AVG wirbt im Reiter Performance für eine weitere App, den AVG Cleaner, welcher weitere Performanceverbesserungen für das Smartphone bringen soll.

Anti-Theft

Der Diebstahlschutz ist standardmäßig nicht aktiviert. Die Steuerung erfolgt über ein Webinterface (https://www.avgmobilation.com/) oder über SMS Kommandos.



Shout

SMS Kommando: AVGShout <Password>

Die Shout Funktion lässt auf dem Smartphone eine Melodie ertönen, die es dem Nutzer ermöglicht ein verlegtes Gerät wiederzufinden. Dabei wird das Gerät nicht gesperrt. Der Alarm kann durch einfaches Tippen deaktiviert werden.

Locate

SMS Kommando: AVGLocate <Password>

Dieses Feature ortet das Gerät aus der Ferne. Im Webinterface wird die Position in einer Karte von Google Maps angezeigt. Bei Ortung per SMS wird ein Link auf eine Karte von Google Maps gesendet, wo die aktuelle Position des Smartphones eingetragen ist. Ein Aufzeichnen des Bewegungsverlaufes wird nicht angeboten.

Lock

SMS Kommando: AVGLock <Password>

Dieses Kommando sperrt das Gerät mit einem Passwort. Im Webinterface kann ein Text angegeben werden, welcher im Falle einer Sperrung am Display angezeigt wird.
Die Sperre war in unserem Test sehr solide und konnte nicht überwunden werden. Ein Kritikpunkt ist, dass es uns nicht möglich war einen Notruf abzusetzen. Dies kann im Falle eines Notfalls gefährlich sein.

Wipe

SMS Kommando: AVGWipe <Password>

Diese Funktion löscht die Daten des Nutzers vom Smartphone, um sie für Dritte unzugänglich zu machen. Ist die App als Device-Administrator gesetzt wird das Gerät hierbei auf Werkseinstellungen zurückgesetzt, was zur Folge hat, dass der Diebstahlschutz anschließend nicht mehr aktiv ist. Hat die App die genannten Rechte nicht werden die Daten gelöscht ohne das Geräte zurückzusetzen. In unserem Test hat dies wie erwartet funktioniert und auch ohne Device-Administrator Rechte wurden alle Daten (nicht SMS) gelöscht.

Camera Trap (PRO)

Die Camera Trap erstellt bei dreimalig falscher Passworteingabe ein Foto mit der Frontkamera des Geräts. Dieses Bild wird dem Nutzer anschließend zusammen mit der Position per Email zugestellt.



SIM Lock (PRO)

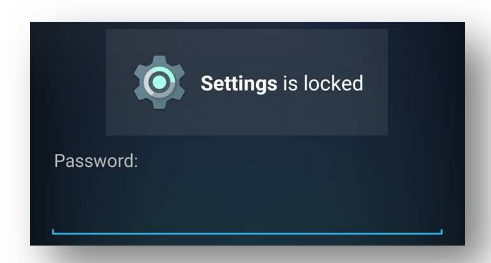
Die SIM Lock Funktion sperrt das Gerät wenn eine fremde SIM Karte in das Gerät eingelegt wird, etwa wenn ein Dieb seine eigene verwenden möchte. Zusätzlich wird der Nutzer per Email, mit zusätzlicher Standortinformation, über diesen Zustand benachrichtigt.

Privacy

Im Reiter Privacy werden nachfolgende Funktionen zusammengefasst, welche die Privatsphäre des Nutzers betreffen.

App Lock (PRO)

Mit App Lock können ausgewählte installierte Apps mit einem Passwort geschützt werden. Ohne gültigem Kennwort kann die jeweilige App nicht genutzt werden.

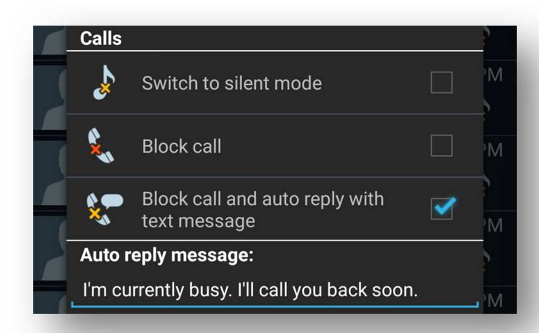


App Backup (PRO)

Das App Backup erstellt Sicherungskopien von installierten Apps. Hierbei ist zu beachten, dass keine App Daten gesichert werden, sondern lediglich die Installationsdateien (APK). Backups werden lokal auf dem Gerät gesichert.

Call Blocker

Der Call Blocker erlaubt es dem Nutzer sich gegen Störenfriede zu wehren. Es ist möglich Anrufer auf stumm zu schalten, abzuweisen oder zu blockieren und automatisch eine Nachricht an den Anrufer zu senden. Letztgenannte kann frei definiert werden. Insgesamt hat die Komponente gut funktioniert.



Eigenartig war das Verhalten nur bei der Stummschaltung von Anrufen. In unserem Test wurde der Benachrichtigungsmodus einfach von „All“ auf „Priority“ gesetzt. Zu bemängeln ist, dass das Gerät anschließend in diesem Zustand bleibt. So könnte der Nutzer legitime Anrufe verpassen.

Updates

Updates werden automatisch alle 24 bis 48 Stunden heruntergeladen. Zudem können Aktualisierungen manuell angestoßen werden.

Hilfe

Es ist keine Offlinehilfe verfügbar. Online werden FAQ geboten, zudem ist es möglich den technischen Support zu kontaktieren.

Deinstallation

Ist die „App Lock“ Funktion aktiviert, so ist es notwendig das Kennwort für die Deinstallation anzugeben.

Lizenz

AVG AntiVirus ist in einer umfangreichen FREE Version gratis erhältlich. Für die Funktionen Camera Trap, App Lock, Device (SIM) Lock und App Backup ist ein Upgrade auf die PRO Version von Nöten. Diese ist für 2,59€ monatlich oder 10,49€ jährlich erhältlich.

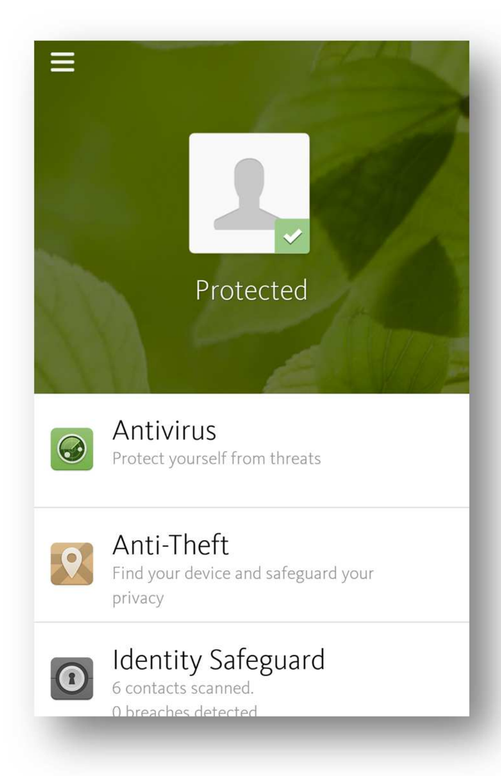
Fazit

AVG bietet ein umfangreiches Sicherheitsprodukt welches auch schon in der FREE Version mit den gut funktionierenden gängigen Funktionen zu überzeugen weiß.



Avira Antivirus Security

Avira Antivirus ist eine umfangreicher Sicherheitsapp die neben Antivirus und Anti-Theft auch noch Funktionen wie App Lock und Blacklisting anbietet. Neu, in dieser Version, ist die Funktion Privacy Advisor welche Apps nach den benötigten Berechtigungen beurteilt und sich derzeit noch im Beta Stadium befindet. Für Nutzer der Pro Version steht zusätzlich noch eine Secure Browsing Komponente zur Verfügung welche den Nutzer aktiv beim Surfen vor Phishing und Malware schützen kann.

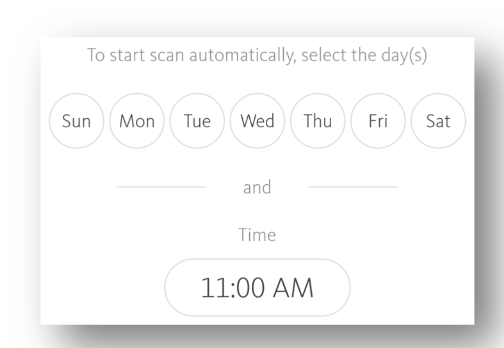


Installation

Avira Antivirus Security wurde aus dem Google Play Store bezogen und installiert. Nach einer kurzen Tour wird der Nutzer aufgefordert ein Konto anzulegen um den vollen Funktionsumfang nutzen zu können. Abschließend wird der Startbildschirm angezeigt und ein initialer Malwarescan durchgeführt.

Antivirus

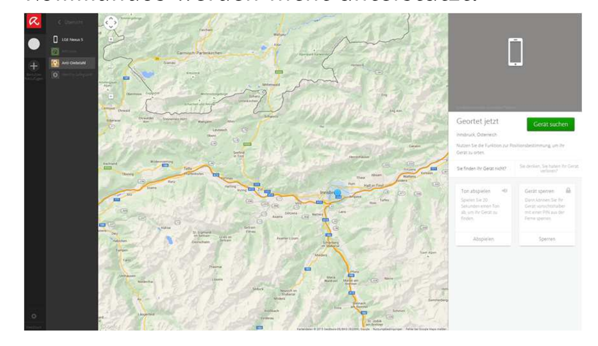
Die Antivirus Komponente überprüft das Gerät auf Schadsoftware. In den Einstellungen kann gewählt werden ob nur Dateien,



nur Anwendungen oder beides gescannt werden sollen. Zudem können zu überprüfende Gefahrenkategorien eingestellt werden. Hier können *Adware* und *PUA* aktiviert und deaktiviert werden. Gefallen hat uns auch, dass Scans automatisiert gestartet werden können. Hierfür können die Tage der Woche, sowie der Zeitpunkt des Scans gewählt werden.

Anti-Theft

Anti-Theft fast Funktionen betreffend dem Diebstahlschutz zusammen. Um den vollen Funktionsumfang nutzen zu können muss Avira als Geräteadministrator eingetragen werden. Die Steuerung der Komponente erfolgt über ein Webinterface (http://my.avira.com). SMS Kommandos werden nicht unterstützt.



Locate

Die Locate Funktion ortet ein verloren gegangenes oder gestohlenes Gerät einmalig und zeigt die Position auf einer Karte von Google Maps an. Eine kontinuierliche Ortung ist nicht möglich.

Yell

Die Yell Funktion lässt für 20 Sekunden eine schrille Sirene ertönen, die beim Wiederfinden des Geräts helfen soll. Das Display wird hierbei nicht gesperrt.



Wipe

Über das Webinterface ist es möglich Daten auf dem Gerät zu löschen. Hierfür können die drei Möglichkeiten „Speicher“, „SIM-Karte“ und „Zurücksetzen auf Werkeinstellung“ beliebig kombiniert werden. Das Löschen der SIM-Karte funktionierte in unserem Test nicht.

Lock

Die Lock Funktion sperrt das Gerät und hindert Unbefugte davor das Gerät zu verwenden. Die Komponente ist im Allgemeinen sehr gut gemacht. Es war uns nicht möglich die Sperre zu umgehen. Außerdem kann ein Text während der Sperre eingeblendet werden. Der Nutzer hat nur drei Versuche für die Eingabe des PINs. Gibt er öfter den Falschen ein, so ist das Gerät dauerhaft gesperrt und kann nur noch per Webinterface entsperrt werden. Bedauerlich ist, dass es nicht möglich ist einen Notruf abzusetzen, was im Ernstfall problematisch sein kann.

Identity Safeguard

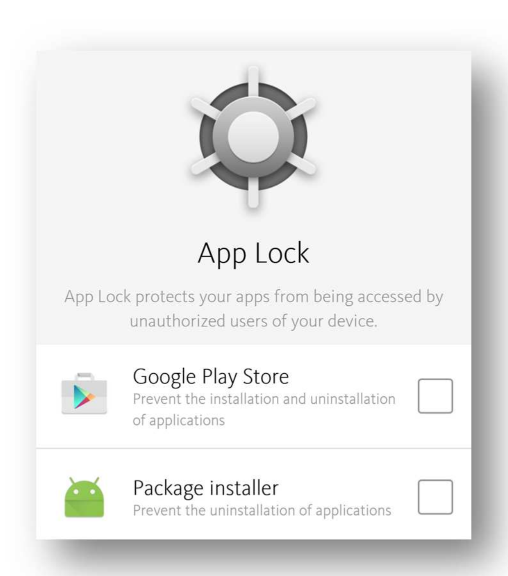
Der Identity Safeguard warnt den Nutzer, wenn seine Emailadresse von großen Datenlecks betroffen ist. In der Vergangenheit war diesbezüglich zum Beispiel Adobe betroffen, wo eine große Anzahl an Datensätzen an die Öffentlichkeit gelangt ist. Avira prüft, ob die Emailadresse des Nutzers, oder eine Emailadresse eines Eintrags in der Kontaktliste, bei einem dieser großen Datenlecks an die Öffentlichkeit gelangt ist.

Secure Browsing

Avira schützt den Nutzer während dem Surfen im Internet vor Phishing und schadhaften Webseiten. Im Falle einer Erkennung scheint ein Popup auf, welches den Nutzer entsprechend auf die Gefahr hinweist.
In unserem Kurztest mit aktuellen Phishingseiten hat die Komponente korrekt gearbeitet.

App Lock

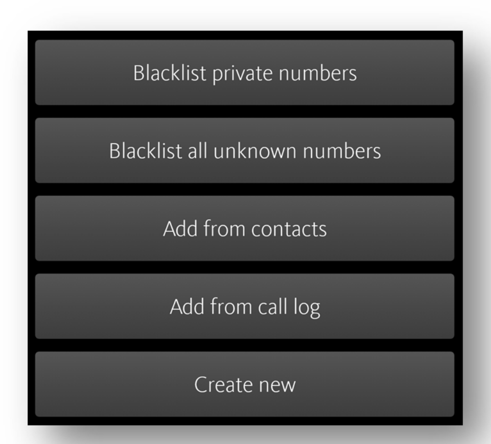
App Lock ermöglicht das Sperren von installierten Apps. Diese lassen sich erst nach Eingabe eines zuvor vergebenen PINs starten.



Dies kann zum Beispiel sinnvoll sein wenn man das Gerät einem Kind überlassen und gewisse Apps von der Verwendung ausschließen möchte. Standardmäßig sind der Google Play Store, Package Installer und die Einstellungen aktiviert. Dadurch wird die Installation und Deinstallation von Apps verhindert.

Blacklist

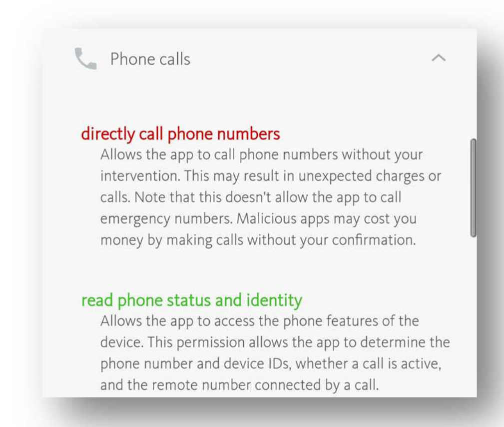
Blacklist erlaubt das Blockieren von zuvor definierten Anrufen. Nummern können vom Adressbuch, den Kontakten oder manuell hinzugefügt werden. Zudem können Anrufer mit unterdrückter Nummer oder unbekannte Nummern generell abgewiesen werden. Obwohl eine Meldung eingeblendet wurde, dass es auf manchen Nexus Geräten zu Problemen kommen kann, hat die Komponente einwandfrei funktioniert.





Privacy Advisor

Der Privacy Advisor ist aktuell im Betastadium verfügbar. Installierte Apps werden in die Kategorien High-, Medium- und Low Risk eingeteilt.



Die Zuordnung erfolgt aufgrund der von den Apps erforderten Berechtigungen. Tippt der Nutzer eine der Apps an, so werden alle vergebenen Berechtigungen samt kurzer Erklärung aufgelistet – schön gemacht.

Avira Optimizer

Der Avira Optimizer ist ein Optimierungstool für Android und ist nicht in der App inkludiert. Es wird lediglich direkt auf den Google Play Store verlinkt.

Updates

Updates werden automatisch täglich durchgeführt. Für Nutzer der PRO Version stehen noch häufigere Aktualisierungen zur Verfügung.

Hilfe

Es ist keine Offlinehilfe verfügbar. Der Nutzer wird auf die mobile Webseite des Herstellers weitergeleitet, wo er FAQ und weitere Hilfestellungen findet.

Deinstallation

Ist der integrierte App Lock aktiviert, so wird für die Deinstallation ein PIN benötigt. Somit können Diebe den Diebstahlschutz nicht einfach deaktivieren. Nachdem die App aus den Geräteadministratoren ausgetragen wurde kann sie deinstalliert werden.

Lizenz

Avira Antivirus Security kann mit eingeschränktem Funktionsumfang kostenlost verwendet werden. Nutzern der PRO Version stehen die Secure Browsing Komponente, kürzere Updateintervalle, sowie technischer Support zur Verfügung.

Fazit

Mit Avira Mobile Security erhält der Nutzer ein ausgereiftes Sicherheitsprodukt welches auch schon in der gratis Version zu überzeugen weis da sie auch hier schon alle gängigen Funktionen einer Sicherheitsapp beinhaltet.



Baidu Mobile Guard

Baidu Mobile Guard ist ein kostenloses Sicherheitsprodukt, welches eine Vielzahl an Funktionen wie Mobile Tuning, App Management, Schutz vor unerwünschten Anrufen und Antivirus bietet.



Installation

Baidu Mobile Guard wurde aus der Chinesischen HIAPK Appstore bezogen und konnte ohne Schwierigkeiten installiert werden.

Frequently used functions

In diesen Tab zeigt Baidu oft verwendete Funktionen an. So werden Zugänge zu Speedupfunktionen, Bereinigung von Trash-Dateien, App Management, Anruf Blocker, Traffic Manager und sicheres Bezahlen angezeigt.

Intitial Check-up

In einer kreisförmigen Anzeige wird dem Nutzer der aktuelle Schutzstatus des Geräts angezeigt. Durch Tippen auf die Mitte des Bildschirms wird ein Tune-Up gestartet, welcher den Speicher bereinigt, Prozesse beendet und Trash-Dateien entfernt.

Smartphone Speedup

Nach dem initialen Checkup bietet die Komponente Smartphone Speedup weitere Möglichkeiten um mehr aus unserem Gerät zu holen. Der Nutzer hat die Möglichkeit laufende Prozesse zu terminieren. Zudem erhalten wir die Empfehlung einer weiteren App welche andere Apps am „aufwecken“ des Geräts hindern soll um sicherzustellen, dass unser Gerät „flüssig“ arbeitet.

Junkfile Cleaner

Junkfile Cleaner löscht Caches von Apps, übriggebliebene Dateien, sowie nicht mehr benötigte Installationsdateien. Zudem werden nicht mehr benötigte Systemdateien entfernt.

In der rechten oberen Ecke erhält der Nutzer Zugriff auf die „Mobile phone cache cleaner“, einer Funktion die Caches leeren und Bilder, Musik und Videos löschen kann, um mehr Speicherplatz auf dem Gerät zu erhalten.

App Management

Das App Management ermöglicht das Deinstallieren und Updaten von installierten Applikationen auf dem Gerät. Zudem können installierte Apps vom internen Speicher auf die externe SD Karte verschoben werden. Außerdem können Installationsdateien verwaltet werden. Zudem können vorinstallierte Apps entfernt werden.

Security

Aus diesem Tab erhält der Nutzer Zugriff auf den Antivirenscanner und das Blockieren von Störenfrieden. Der „Super Mode“ erfordert Root Berechtigungen und bietet die Deinstallation von Apps, welche auf dem Gerät bereits werksseitig vorinstalliert wurden und sich in der Regel nicht entfernen lassen.





Fraud Protection

Mit Hilfe dieser Funktion kann der Nutzer bis zu drei Familienmitglieder vor Telefonbetrug schützen. Es müssen die Telefonnummern der zu schützenden Geräte angegeben werden. Diese erhalten dann jeweils einen Link zum Baidu Mobile Guard.

Disturbance Blocker

Spam SMS und Werbeanrufe sind nach wie vor ein großes Problem in China. Der Disturbance Blocker soll vor derartigen Problemen schützen. In unserem Test wurden Festnetznummern korrekt als Werbeanruf identifiziert.

Payment Protection

Diese Komponente stellt eine sichere Umgebung für Internetzahlungen bereit, etwa durch das Scannen auf gefälschte Apps, den Sicherheitsstandard des WIFI und das Schützen von SMS.

Innerhalb der App kann der Nutzer ein Versicherung von CNY 6000 pro Überweisung, mit einem jährlichen Limit von CNY 100.000 abschließen.

AV Scanner

Über dieses Menü kann der Nutzer direkt einen Antivirenscan starten. Eine vollständige Überprüfung kann nur aus diesem Menü angestoßen werden. Malwaredefinitionen werden automatisch aktualisiert. Die Unterstützung durch die Cloud ist standardmäßig aktiviert, ebenso die Überprüfung während der Installation von Apps.

Find out more

Hier findet der Nutzer ein Tool zum sicheren Verbinden zu WiFi Netzwerken („WiFi Radar"), eine weitere Tune-Up Funktion zum Entfernen von nicht mehr benötigten Dateien und den Zugang zu Baidus Suchmaschine.



Baidu Astronaut

Nach der Installation der Baidu App wurde auf dem Desktop ein kleines Icon angezeigt. Durch Ziehen des Buttons in die Mitte des Bildschirms wird ein kleiner Astronaut angezeigt. Dieser soll die Durchführung eines Quick Cleanups visualisieren. Anschließend wird ein Report angezeigt.



Deinstallation

Es wird kein Deinstallationsassistent angeboten. Wie auch schon im Vorjahr wird für die Deinstallation kein Password benötigt.

Lizenz

Baidu Mobile Manager ist kostenlos verfügbar.

Hilfe

Es wird innerhalb der App Hilfe angeboten.

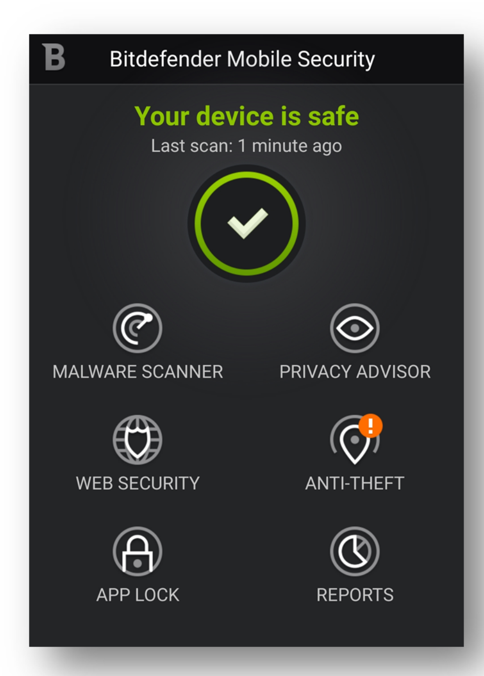
Fazit

Baidu Mobile Guard ist ein einfach zu verwendendes Sicherheitsprodukt, welches ein Vielzahl an Funktionen mitbringt. Natürlich steht es jedem Hersteller frei weitere Standalone-Apps zur Installation zu empfehlen. In unseren Augen gilt dies nur für Apps mit echtem Mehrwert. Baidu sollte darauf achten es nicht mit derartigen Empfehlungen zu übertreiben. Außerdem sehen wir die Empfehlung das Gerät zu rooten als sehr kritisch. Auch in diesem Jahr bietet Baidu keinen Diebstahlschutz an.



Bitdefender Mobile Security & Antivirus

Bitdefender bietet neben der Malware und Anti-Theft Komponente noch umfangreiche Funktionen wie etwa App Lock und den Privacy Advisor.



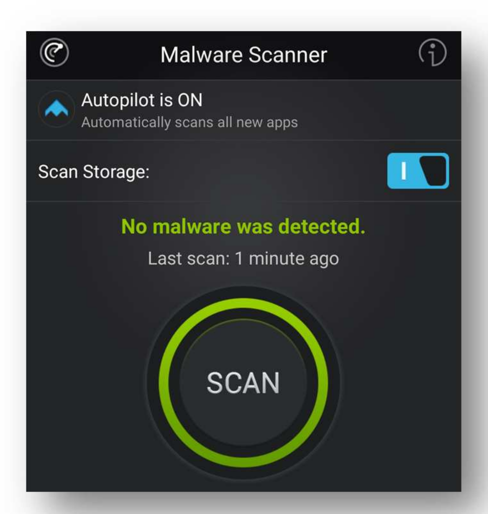
Installation

Bitdefender Mobile Security & Antivirus wurde aus dem Google Play Store bezogen und installiert. Nach dem Akzeptieren der EULA muss sich der Nutzer mit seinem Bitdefender Account einloggen, oder einen solchen erstellen. Alternativ kann auch einfach der Google Account verwendet werden. Abschließend muss das Produkt lizensiert werden. Es kann entweder eine 14-tägige Testversion gestartet, eine Lizenz erworben, oder ein bestehender Produktschlüssel eingegeben werden.

Malware Scanner

Der Virenscanner bietet dem Anwender die Möglichkeit, die installierten Apps und den Speicher des Mobiltelefons auf Malware zu überprüfen. Die Überprüfung des Speichers ist hierbei optional, die installierten Apps werden bei jedem Durchlauf gescannt. Diese werden auch automatisch während der Installation gescannt.

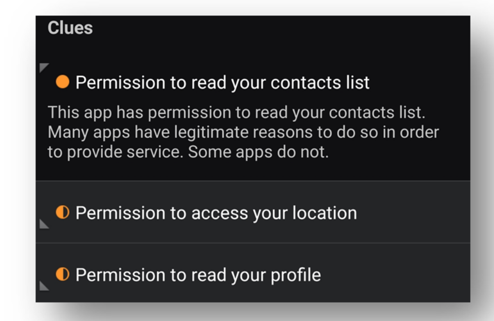
Der Malware Scanner funktioniert nur mit bestehender Internetverbindung, da die Cloud für die Erkennung herangezogen wird.



Privacy Advisor

Der Privacy Advisor analysiert installierte Apps auf mögliche Verletzungen der Privatsphäre. Um den Nutzer nicht mit Details zu überfluten gibt Bitdefender eine Punktezahl zwischen 0 und 100 an, um die gesamte Sicherheitssituation zu bewerten. Je niedriger die Zahl ist, umso mehr Apps mit fragwürdigen Berechtigungen wurden erkannt.

Des Weiteren werden alle installierten Applikationen aufgelistet. Durch Antippen eines Eintrags werden alle Berechtigungen detailliert aufgeschlüsselt.



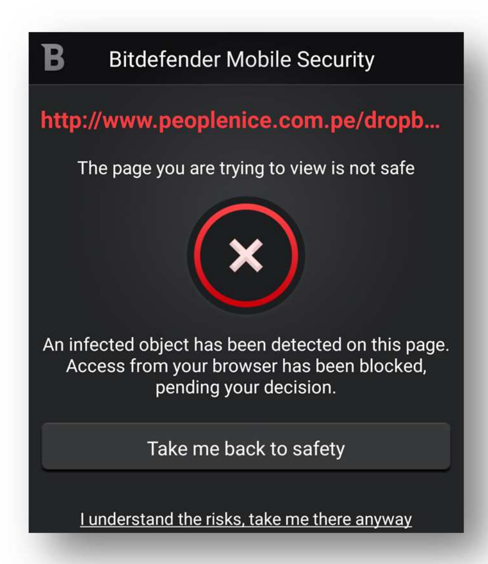
Dies wurde unserer Meinung nach auch gut umgesetzt. Es werden für jede App die erforderten Berechtigungen gelistet und mit einem Ampelsystem bewertet. Zudem gibt



Bitdefender zu jeder Berechtigung eine kurze Erklärung ab.

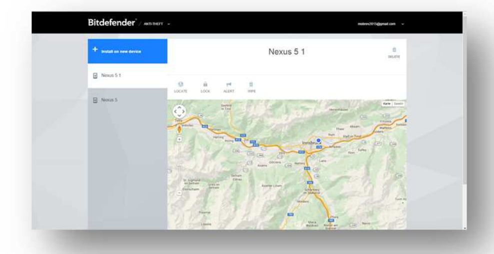
Web Security

Web Security schützt den Nutzer während dem Surfen im Internet vor gängigen schadhaften Angriffen. Bitdefender gibt an vor Phishing, Betrug und Malware zu Schützen.



Anti-Theft

Der Diebstahlschutz von Bitdefender kann entweder über ein Webinterface (http://my.bitdefender.com), oder SMS Kommandos gesteuert werden. Dazu muss die Applikation als Geräteadministrator eingetragen werden um ihr ausreichend Privilegien für die Durchführung von Lösch- und Sperrkommandos zu gewähren. Bitdefender gibt gleich den Hinweis, dass vor der Deinstallation der Applikation die Geräteadministratorberechtigung deaktiviert werden muss. Um den Vorgang abzuschließen muss ein vier- bis achtstelliger PIN vergeben werden.



Zusätzlich muss ein vertrauenswürdiger Freund eingetragen werden. Dieser wird benachrichtigt wenn die SIM Karte gewechselt wird, und ist die einzige Nummer von der das Wipe-Kommando akzeptiert wird. Gefallen hat uns, dass zu jeder einzelnen Komponente ein erklärender Hilfetext eingeblendet wird.

Locate

SMS Kommando: BD-<PIN> LOCATE

Die Locate Funktion lokalisiert das Gerät. Im Webinterface wird die Position in eine Karte von Google Maps eingetragen. Die Möglichkeit einer kontinuierlichen Ortung zum Aufzeichnen des Bewegungsprofils besteht nicht.
Bei Verwendung von SMS Kommandos wird an den Absender eine Antwort mit einem Link auf eine Karte von Google Maps gesendet.

Scream

SMS Kommando: BD-<PIN> SCREAM

Die Scream Funktion lässt auf dem Gerät eine schrille Sirene ertönen. Dabei wird es nicht gesperrt.

Lock

SMS Kommando: BD-<PIN> LOCK

Dieser Befehl sperrt das Gerät und schützt somit vor unbefugtem Zugriff. Dabei setzt Bitdefender auf den in Android integrierten Sperrbildschirm. Dieser ermöglicht zwar nicht das Platzieren von Nachrichten oder Logos, dafür gibt es keinerlei Beanstandungen bezüglich der Sicherheit. Es ist nicht möglich ihn zu umgehen, außerdem kann jederzeit ein Notruf abgesetzt werden. Wird der Befehl mittels SMS abgesetzt, so kann das Gerät mit dem zuvor angegebenen Anti-Theft PIN entsperrt werden. Über das Webinterface kann ein vierstelliger PIN frei vergeben werden.

Probleme sehen wir bei der Verwendung der Funktion mit SMS. Bei der getesteten Android Version werden SMS standardmäßig am Sperrbildschirm angezeigt, wodurch ein Dieb den PIN in Erfahrung bringen kann. Dramatisch wäre dies nicht, wenn man für den Sperrbildschirm einen anderen PIN oder ein Lock-Pattern vergeben könnte. Bitdefender



überschreibt bestehende Sicherheitsfeatures jedoch einfach, wodurch ein Zugriff auf das Gerät kinderleicht wird. Abhelfen kann sich ein Nutzer nur indem er in den Einstellungen sämtliche Notifications auf dem Sperrbildschirm deaktiviert. Auf diesen Zustand macht Bitdefender jedoch nicht aufmerksam. Zusätzlich ist es auch hier möglich auf den Gast-User Account zu wechseln.

Wipe

SMS Kommando: BD-<PIN> WIPE

Die Wipe Funktion löscht persönliche Daten vom Gerät des Benutzers. Hierfür wird das Smartphone auf Werkseinstellungen zurückgesetzt. Dieses Kommando kann als SMS nur von der vertrauenswürdigen Nummer versandt werden.

Callme

SMS Kommando: BD-<PIN> CALLME

Diese Funktion kann nur mithilfe von SMS Kommandos ausgeführt werden. Nach Absetzen des Kommandos wird der Absender des SMS angerufen und der Anruf auf dem Gerät versteckt. Ein Bestohlener kann so den Dieb heimlich belauschen. Zudem wird der Lautsprecher aktiviert, wodurch zum Beispiel ein ehrlicher Finder kontaktiert werden kann.

SIM Change

Die SIM Change Funktion benachrichtigt die vertrauenswürdige Nummer wenn eine fremde SIM Karte eingelegt wird. In unseren Tests hat diese Komponente nicht funktioniert.

App Lock

App-lock ermöglicht einen Passwortschutz von installierten Apps. Der Nutzer kann einstellen, für welche Apps ein Passwort erforderlich sein soll. So kann etwa definiert werden, dass für das Öffnen der Galerie ein PIN eingegeben werden muss. Dies kann etwa auch hilfreich sein um Kindern den Zugriff zu gewissen Funktionen zu verhindern.

Updates

Da Bitdefender keinen offline Malwarescan anbietet, sondern stets die Bitdefender Cloud für die Überprüfung von Dateien verwendet, sind Updates obsolet.

Hilfe

Bitdefender bietet dem Nutzer am Smartphone keine explizite Hilfe an. Für jede Funktion existiert allerdings eine kurze, jedoch nützliche Kurzinformation.

Deinstallation

Für die Deinstallation von Bitdefender ist der zuvor eingegebene PIN notwendig. Dies ist sinnvoll, denn so kann ein Dieb nicht einfach den Diebstahlschutz deaktivieren.
In unserem Test konnten wir feststellen, dass zwar das Eingabefeld für den PIN eingeblendet wird und erst auch sicher erschien, jedoch konnten wir nach etwa 30 Sekunden probieren die Eingabemaske umgehen und das Produkt ohne PIN Eingabe deinstallieren. Hier muss nachgebessert werden.

Lizenz

Bitdefener Mobile Security & Antivirus kann 14 Tage lang gratis getestet werden. Danach kann eine Lizenz erworben werden. Hierfür steht eine Monatliche Zahlung für €0,99 oder ein Jahres Abo für €9,95 zur Auswahl.

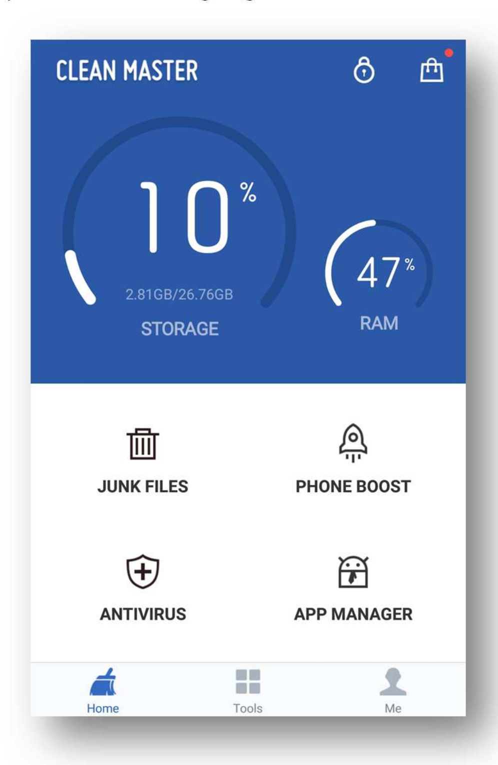
Fazit

Bitdefender bietet ein umfangreiches Sicherheitsprodukt welches einen sauberen Eindruck hinterlässt. In unserem Test funktionierten aber manche Funktionen leider nicht zufriedenstellend. Im Falle der SIM Change Funktion erhielten wir auch nach mehrmaligen testen keinen Warn-Nachricht provozieren.



Cheetah Mobile Clean Master

Cheetah Mobile Clean Master ist eine umfangreiche Antivirus und Performance App welche im Gegensatz zu anderen umfangreichen Produkten aber über keine Anti-Theft Komponente verfügt. Clan Master bietet hingegen eine Vielzahl von Tools um die Performance des Gerätes zu verbessern wie z.B. das Löschen von Junk Files um den Speicher zu bereinigen. Erwähnenswert ist auch die Foto-Backup Funktion welche gratis 2Gb Cloud Speicher zu Verfügung stellt.



Installation

Cheetah Mobile Clean Master wurde aus dem Google Play Store bezogen und installiert. Die Installation erforderte keine weitere Konfiguration. Der Nutzer wird auf den Startbildschirm weitergeleitet.

Junk Files

Diese Funktion findet nicht benötigte Dateien, wie zum Beispiel Cache Dateien, im lokalen Dateisystem. Dem Nutzer wird angeboten diese Dateien zu löschen und das System so zu bereinigen. Unser Gerät, welches bis jetzt nur für ein paar wenige Tests verwendet wurde, wies laut Clean Master bereits einen Umfang von 528MB Junkfiles auf. Unter den zu löschenden Daten befanden sich obsolete APK Dateien, nicht mehr benötigte Daten im Telefonspeicher, sowie Dateien die im Cache liegen. Nach dem Abschluss der Aktion wird das Ergebnis eingeblendet, sowie Empfehlungen zur Installation weiterer Produkte von CM angezeigt.

Phone Boost

Die Phone Boost Funktion bereinigt den Arbeitsspeicher von überflüssigen Daten laufender Applikationen. In unserem Test wurden etwa Apps wie die Uhr oder Media Storage angezeigt. Zusätzlich werden Apps wie Google Drive angezeigt, wofür jedoch eine Empfehlung gegeben wird die Daten im RAM zu belassen. In unserem Test konnten 23MB an Daten aus dem RAM entfernt werden. Zusätzlich wird auf eine erhöhte CPU Temperatur verwiesen, welche mit dem CPU Cooler heruntergesetzt werden kann, siehe Abschnitt „CPU Cooler“.

Antivirus

Die Antiviruskomponente des Produkts untersucht das Gerät nach möglichen Problemen, die die Sicherheit betreffen können. Die bloße Überprüfung des Dateisystems und installierten Apps nach Malware ist für Cheetah Mobile jedoch nicht genug. So wird zum Beispiel angeführt, dass Apps installiert sind, welche auf die Kontakte zugreifen können, welche geschützt werden sollten. Als Lösung wird die Installation von CM Security empfohlen. Zudem wird die Aktivierung von CM AppLock empfohlen, was den Zugriff auf Apps verhindern soll.





Durch Tippen auf den Kontextmenüeintrag „Privacy" können Probleme behoben werden, welche die Privatsphäre des Nutzers betreffen können. Konkret wird das Clipboard geleert, zudem wird der Nutzer auf eine Maske weitergeleitet von wo aus die manuelle Bereinigung von privaten Daten durchgeführt werden kann, wie z.B. den SMS.

App Manager

Im Appmanager werden installierte Anwendungen nach unterschiedlichen Kriterien aufgeschlüsselt gelistet. Apps können direkt deinstalliert oder lokal gesichert werden. Clean Master zeigt sich in dieser Ansicht weitaus weniger bissig als im letztjährigen Test. Während uns letztes Mal empfohlen wurde sämtliche Browser zu deinstallieren um sie mit dem CM Browser zu ersetzen erhalten wir diesmal lediglich eine Ansicht, die redundante Apps aufzeigt.

Am Ende der Liste der installierten Apps werden anschließend duzende weitere, empfohlene Apps angezeigt. Durch Wischen nach rechts wechselt das Userinterface zu den „Picks", einem Appstore wo besonders beliebte Apps gelistet werden.

In einer weiteren Tab-Seite werden APK Dateien gelistet, welche im Dateisystem gefunden wurden. Hierbei steht die Entfernung der Datei im Vordergrund, auch wenn es möglich ist in der Detailansicht die APK Datei auszuführen und somit zu installieren.

Eine weitere Funktion des Appmanagers ist es, Daten von Apps vom internen Speicher auf den externen zu verschieben. Dies kann sinnvoll sein, wenn der interne Speicher sehr begrenzt ist, jedoch eine große SD Karte im Gerät verfügbar ist.

CPU Cooler

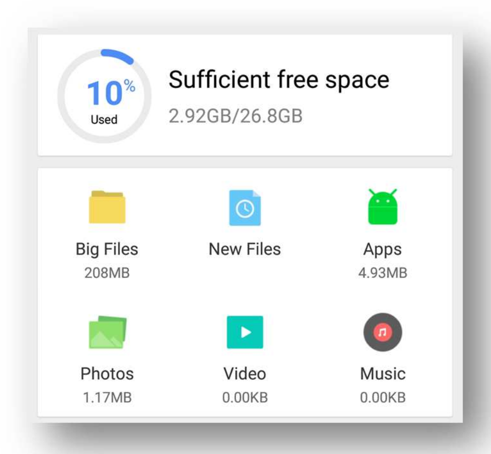
Der CPU Cooler überwacht den Prozessor auf überhöhte Temperatur und ermöglicht durch Schließen geöffneter Apps eine Abkühlung. In unserem Test wurde angegeben, dass die Temperatur um 1 Grad Celsius gesenkt werden konnte. Der Nutzer muss selbst entscheiden wie nützlich diese Funktion für ihn ist.

Photo Manager

Der Photomanager sucht Bilder auf dem Smartphone des Nutzers. In einer Ansicht mit Vorschaubildern kann der Nutzer dann ausgewählte Fotos löschen.

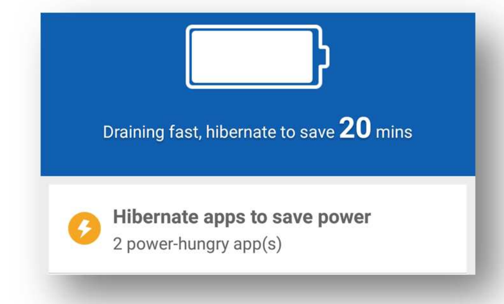
Space Manager

Der Space Manager sucht unterschiedliche Dateitypen auf dem Smartphone und schlüsselt sie nach Kategorien auf. So ist es etwa möglich sehr große Files in einer Liste anzuzeigen um sie gegebenenfalls zu entfernen.



Battery Saver

Der Battery Saver kann laufende Apps in einen Hibernate Zustand versetzen um die Batterielaufzeit zu verlängern. In unserem Test wurden zwei Apps gelistet, die angeblich die Batterielaufzeit um 20 Minuten verkürzen.



AppLock

AppLock erlaubt es installierte Apps mit einem Sperrmuster zu schützen. Dieses muss



eingegeben werden bevor die zu schützende App gestartet wird. Gefallen hat uns, dass bei mehrmaliger falscher Eingabe des Musters ein Foto mit der Frontkamera aufgenommen wird.

Check Network Traffic

Der Network Traffic Checker listet Apps mit der jeweiligen Datennutzung. Zudem wird empfohlen ein weiteres App von CM zu installieren, CM Data Manger, welcher erweiterte Netzwerkmonitor Komponenten enthält.

Downloadmanager

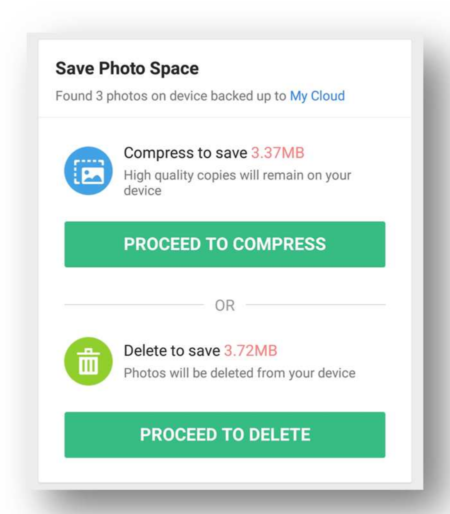
Der Download Manager listet heruntergeladene Dateien, etwa durch Google Chrome, in einer übersichtlichen Ansicht. Es ist möglich nach Datum zu sortieren und Dateien gegebenenfalls zu löschen.

Safe Browsing

Safe Browsing schützt den Nutzer während dem Surfen im Internet und ist standardmäßig in den Einstellungen deaktiviert. In unserem Kurztest mit Google Chrome konnten wir bei aktuellen Phishingseiten keine Erkennung provozieren.

Back Up Photos

Nach der Registrierung eines CM Account wird dem Nutzer 2GB Cloud Speicher kostenlos zur Verfügung gestellt und ermöglicht die Sicherung von Fotos. Die Komponente hat verlässlich gearbeitet.



Nach Abschluss des Vorgangs empfiehlt CleanMaster die Fotos auf dem Gerät entweder zu komprimieren oder gleich zu löschen um Speicherplatz zu sparen.

Updates

Updates können manuell durchgeführt werden. Die App selbst wird über den Google Play Store aktualisiert.

Hilfe

Es werden umfangreiche FAQ innerhalb der App geboten.

Deinstallation

Clean Master kann ohne Passworteingabe mit Hilfe des systeminternen App Managers deinstalliert werden. Da das Programm keinen Diebstahlschutz bietet sehen wir hier keine Probleme.

Lizenz

Clean Master ist gratis im Play Store erhältlich, die App finanziert sich über die Werbung die in der App angezeigt wird.

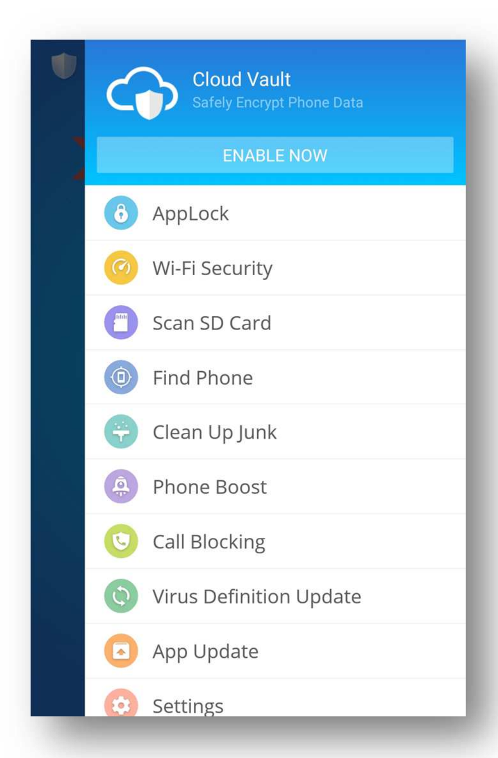
Fazit

Mit CleanMaster erhält der Nutzer eine umfangreiche App welche neben dem Malwareschutz umfangreiche Tools von Speicherbereinigung bis Foto Backup bietet.



Cheetah Mobile CM Security Antivirus

CM Security Antivirus AppLock ist ein weiteres umfangreiches Produkt von Cheetah Mobile. Im Gegensatz zu CleanMaster existiert hier eine Anti-Theft Komponente, welche sich hinter dem Menüpunkt "Find Phone" verbirgt. Dafür wird hier auf einige Performancefunktionen verzichtet, es wird allerdings in der App auf die Installation von CleanMaster verwiesen.



Installation

CM Security Antivirus Applock wurde aus dem Google Play Store bezogen und installiert. Der Installationsvorgang beinhaltet nur die Entscheidung ob man am „User Experience Program" teilnehmen möchte. Anschließend ist der Vorgang abgeschlossen und der Nutzer wird auf den Startbildschirm weitergeleitet.

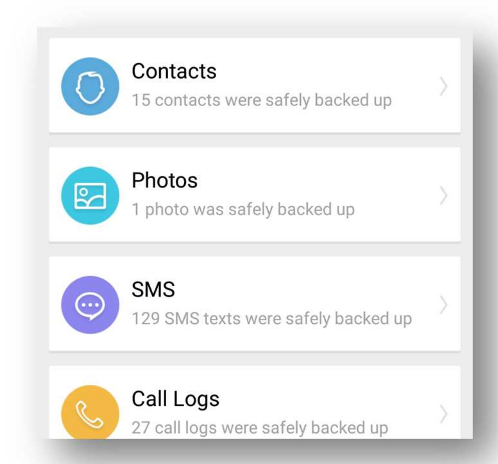
Scan Apps & System

Der Scanner von CM Security überprüft das Gerät auf Schadsoftware. Hier werden standardmäßig lediglich installierte Apps geprüft. Über einen eigenen Menüpunkt kann zusätzlich die SD Karte und der interne Speicher untersucht werden. Andere Verwundbarkeiten, wie installierte Apps die besonders viele Berechtigungen erfordern werden im Ergebnis ebenso berücksichtigt. CM Security empfiehlt zudem den Browserverlauf zu leeren.

Neben den Sicherheits- und Privacy Untersuchungen nimmt CM Security die Systemperformance unter die Lupe. So wurden in unserem Test insgesamt 927MB an Junkdateien gefunden, die automatisch entfernt werden können.

Cloud Vault

Cloud Vault sichert persönliche Daten in die Cloud von Cheetah Mobile. Hierfür werden dem Nutzer zwei Gigabyte an Speicher kostenlos zur Verfügung gestellt. Es können Kontakte, Bilder, SMS und Call Logs gesichert werden. Um die Funktion verwenden zu können muss sich der Nutzer mit seinem Account anmelden oder einen solchen anlegen. Zudem muss die Komponente „Find Phone" aktiviert sein.



Cloud Vault ist übersichtlich gestaltet. Die Sicherung der jeweiligen Daten klappt problemlos. Sollten Daten vom Gerät versehentlich gelöscht werden, so können diese über eine „Restore" Funktion rückgesichert werden. Dies hat in unseren Tests auch mit den SMS funktioniert. Hierfür muss CM Security für kurze Zeit als Standard-SMS-App gewählt werden. Nach erfolgreichem Rücksichern wird Hangouts wieder als Standardapp eingetragen.



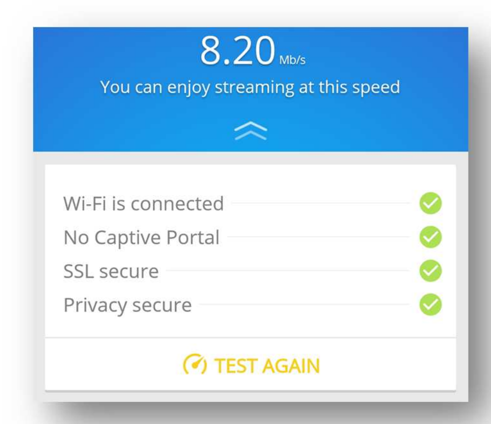
AppLock

AppLock ermöglicht die Vergabe eines Sperrmusters, welches vor dem Start einer Apps eingegeben werden muss. CM empfiehlt Facebook, Google+ und Youtube zu schützen, nicht jedoch die Email App oder die Einstellungen. Diese können vom Nutzer jedoch manuell geschützt werden.

Sollte ein unautorisierter Nutzer beim Versuch ein App zu starten das falsche Muster eingeben, so kann mit der Frontkamera ein Foto erstellt werden. Im Zuge der AppLock Komponente findet sich auch eine „Uninstall Protection". Diese schützt nicht nur das Security Produkt selbst, sondern alle auf dem Gerät installierten Applikationen. Zudem kann eingestellt werden, dass für die Aktivierung von Bluetooth und WiFi das Sperrmuster eingegeben werden muss.

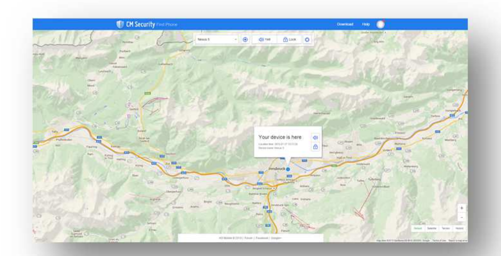
Wi-Fi Security

Wi-Fi Security nimmt das verbundene WLAN Netz unter die Lupe. Es wird untersucht ob ein Captive Portal (Loginseite wie z.B. in Hotels verwendet) installiert ist und ob das Netzwerk SSL und Datenschutz technisch sicher ist. Zudem wird die Downloadgeschwindigkeit erhoben.



Find Phone

Unter diesem Menüpunkt findet der Nutzer den Diebstahlschutz. Bei der erstmaligen Einrichtung muss das Gerät einem Nutzerkonto hinzugefügt werden. Die Komponente wird über ein Webinterface gesteuert (http://findphone.cmcm.com). SMS Kommandos sind nicht verfügbar.



Locate

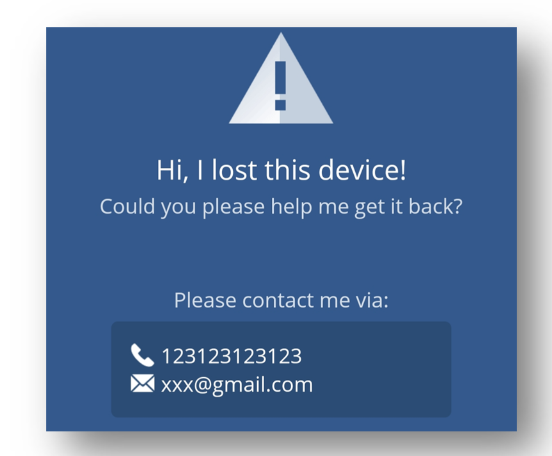
Diese Funktion lokalisiert das Gerät und zeigt die Position in einer Google Maps Karte an. Beim ersten Öffnen des Webinterfaces wird das Gerät automatisch geortet.

Yell

Dieses Kommando lässt auf dem Gerät für 60 Sekunden eine schrille Sirene ertönen. Dabei wird es nicht gesperrt. Dies kann zum Beispiel hilfreich sein um ein verlegtes Gerät wiederzufinden.

Lock

Mit dem Lock Befehl wird das Gerät mit dem zuvor festgelegten Sperrmuster gesperrt. Dies ist insgesamt sehr solide ausgeführt, wir konnten die Sperre nicht umgehen. Zusätzlich fanden wir es sehr gut, dass wir sowohl Telefonnummer, als auch Emailadresse angeben können, die es einem ehrlichen Finder erleichtern sollen ein gestohlenes Gerät zurückzugeben.





Makellos ist der Sperrbildschirm jedoch nicht. So kann kein Notruf mehr abgesetzt werden, was im Notfall sehr problematisch sein kann. Gut gelöst war, dass nach mehrmaliger Falscheingabe der Bildschirm für eine Minute gesperrt ist. Dies erschwert Brute-Force Attacken.

Wipe

Obwohl auf dem Gerät in den erweiterten Einstellungen ein Haken für das Löschen aus dem Webinterface gesetzt werden kann und in der Onlinehilfe auf eine Wipe Funktion verwiesen wird konnten wir diese im Webinterface nicht finden. Cheetah Mobile bestätigte uns, dass sich diese Funktion noch in der Testphase befinde und den meisten Benutzern nicht angezeigt wird.

SIM Alert

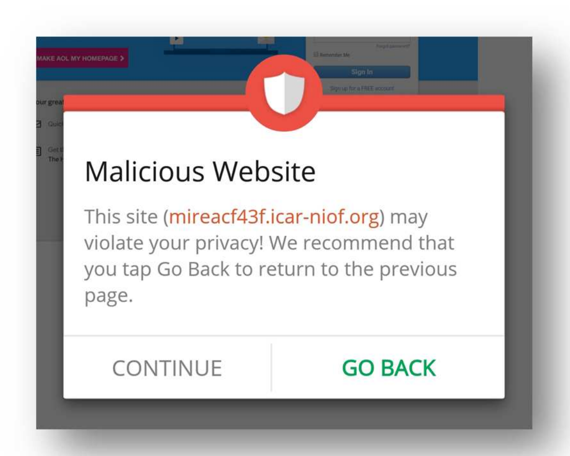
Diese Funktion sendet ein Email an den Nutzer sobald ein Wechsel der SIM Karte durchgeführt wird ein Sperren des Gerätes ist nicht vorgesehen. In unserem Test erhielten wir bei einem SIM Wechsel, auch nach mehreren Versuchen, keine Email. Cheetah Mobile bestätigte nach Rücksprache das Problem und Kündigte an dies mit der nächsten Version zu beheben.

Clean Up Junk

Beim ersten Versuch diese Komponente zu starten werden wir aufgefordert diese nachzuinstallieren. Nach Bestätigung wird der Nutzer auf den Google Play Store weitergeleitet, zur Applikation „Clean Master" von Cheetah Mobile (Siehe auch Cheetah Mobile Clean Master - Insofern werden wir die detaillierte Beschreibung hier überspringen).

Safe Browsing

Ganz unscheinbar (nur ein Schaltknopf in den Einstellungen) liefert Cheetah Mobile eine Safe Browsing Funktion mit. Vor welchen Gefahren CM Security genau schützt konnten wir nicht herausfinden.



In unserem Kurztest mit URLs zu Phishingseiten hat diese auch einwandfrei funktioniert.

Call Blocking

Diese Komponente kann die Anrufe von bestimmten Nummern unterdrücken. Hierfür muss der Nutzer angeben, welche Nummern blockiert werden sollen (Blacklisting). Nummern können entweder manuell eingegeben oder aus den Kontakten und Anruflogs importiert werden.
In unseren Tests hat diese Komponente gut funktioniert. Achtung jedoch beim Format der Telefonnummer bei manueller Eingabe. Die Komponente blockt den Anruf nur, wenn das Format mit Ländervorwahl, jedoch ohne führenden Nullen angegeben wird (z.B. 43699123…).

Updates

Virusdefinitionen können manuell aktualisiert werden. Diese können auch automatisch in nicht näher spezifizierten Zeitabständen erneuert werden.

Hilfe

Die Hilfe ist sehr spärlich. Einzig beim Diebstahlschutz sind einige wenige FAQ angeführt.



Deinstallation

Die App kann über die Android interne Anwendungsverwaltung deinstalliert werden. Hierfür ist keine Passworteingabe notwendig. Dies kann ein Problem sein, denn ein Dieb könnte so den Diebstahlschutz einfach deaktivieren.

Lizenz

CM Security ist gratis aus dem Play Store installierbar.

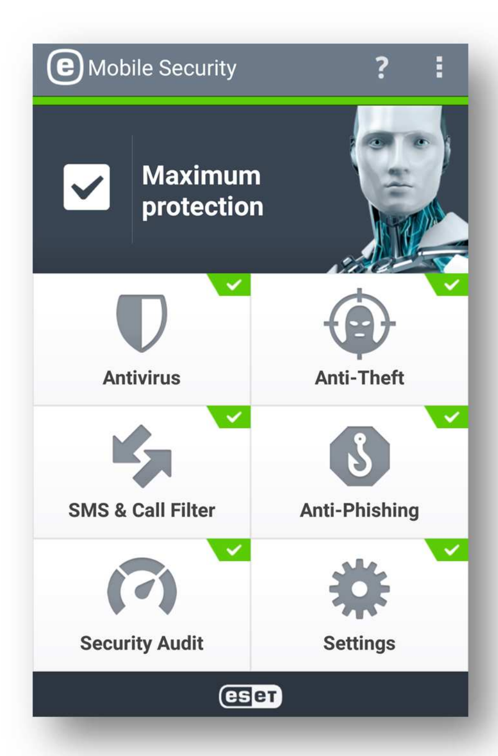
Fazit

Mit CM Security Antivirus AppLock erhält der Nutzer eine ausgereifte Sicherheitsapp die neben der Malware und Anti-Theft Komponente noch über App Lock, Backup und Anruffilter verfügt. Zusätzlich bietet sie mit ihrer Safe Browsing Komponente auch aktiven Schutz beim Surfen im Internet. Einzig die sich noch im Test befindliche Wipe Funktion vermisst man im Vergleich zu anderen Apps.



ESET Mobile Security

ESET Mobile Security ist ein vollständiges Mobile Security Produkt welches neben Antivirus und Anti-Theft in der Pro Version auch die Funktionen SMS & Call Filter und Anti-Phishing bietet. Zusätzlich kann, in der Pro Version, das System noch auf etwaige sicherheitsspezifische Konfigurations-Schwächen durchsucht werden.



Installation

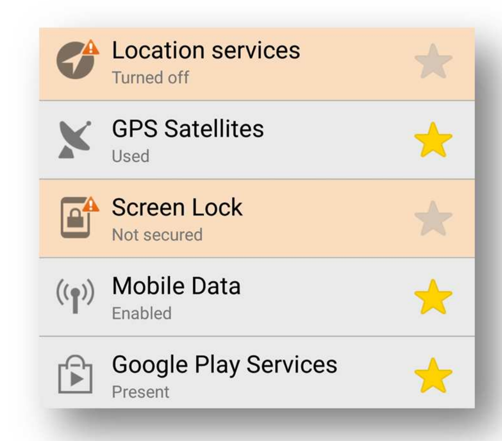
ESET Mobile Security wurde aus dem Google Play Store bezogen und installiert. Im Zuge des Installationsvorganges kann die Sprache und die Region gewählt werden. Zudem kann der Nutzer entscheiden, ob er Teil des ESET Smart Grids sein möchte, einem Frühwarnsystem für Gefahren, welches Daten von Teilnehmern sammelt und höheren Schutz bieten soll. Abschließend kann der Nutzer entscheiden ob PUA blockiert werden soll oder nicht. Abschließend wird der Startbildschirm angezeigt wo im oberen Teil des Bildschirms werden ein Haken und eine Statusmeldung „Maximum protection" eingeblendet wird. Dies könnte einen falschen Eindruck vermitteln, denn bis auf die Antivirus- und Anti-Phishingkomponente sind alle enthaltenen Funktionen inaktiv.

Antivirus

Die Antivirus Funktion bietet die Möglichkeit das System auf Malware zu scannen. Hierfür ist es möglich die Tiefe des Scans einzustellen. Zusätzlich zu manuellen Scans können automatische Scans definiert werden. Sinnvoll ist auch die Funktion „On-Charger Scan", welche automatisch beim Anstecken des Ladegerätes einen Scan startet. Außerdem können Einstellungen bezüglich Echtzeiterkennung und ESET Live-Grid sowie Standardaktionen bei Malwarefunden gesetzt werden. Für Letzteres werden die Aktionen „Entfernen" und „Quarantäne" angeboten.

Anti-Theft

Beim ersten Start der Anti-Theft Komponente muss diese aktiviert werden. Hierfür bietet ESET einen komfortablen Assistenten an. Nachdem ein Passwort festgelegt wurde, wird das App als Geräteadministrator registriert. Im Anschluss wird die aktuelle SIM-Karte als vertrauenswürdige SIM eingetragen. Zudem muss die Nummer eines Freundes gespeichert werden. Gefallen hat uns, dass der Anzeigetext bei gesperrtem Gerät angegeben werden kann. Um SMS Kommandos verwenden zu können wird ein Passwort benötigt. Es wird empfohlen dafür ein eigenes Kennwort zu verwenden. Abschließend muss für die Verwendung des Webinterfaces ein Account erstellt werden.

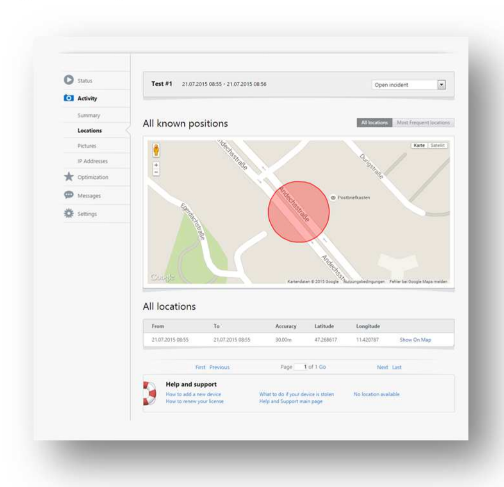


Nach dem Abschluss des Vorgangs wird das Menü von Anti-Theft angezeigt. Der Eintrag



„Optimization“ sticht hervor, da er orange hinterlegt wurde und mit einem Ausrufezeichen darauf hinweist, dass es ein Problem gibt. In unserem Test wurde bemängelt, dass kein Sperrbildschirm aktiviert sei.

Alle Befehle für Anti-Theft können per SMS oder per Webinterface (http://my.eset.com) abgesetzt werden. Im Webinterface muss das Gerät als „vermisst“ gemeldet werden um auf die Diebstahschutzfunktionen zugreifen zu können. Dies leitet automatisch alle wichtigen Schritte ein, welche im Fall eines Diebstahls durchzuführen sind: Sperren, Lokalisieren und Fotos mit der Frontkamera erstellen – jeweils in regelmäßigen Abständen.



SIM Guard

Diese Funktion soll vor unbefugtem Wechsel der SIM-Karte schützen. Wird eine SIM-Karte eingelegt, die nicht hinterlegt ist, wird das Smartphone gesperrt. Diese Funktion hat in unseren Tests einwandfrei funktioniert und wir hatten immer noch die Möglichkeit durch Eingabe des Sicherheits-Passwortes die Sperre aufzuheben oder Notrufnummern zu wählen. Zudem wird die vertrauenswürdige Nummer benachrichtigt.

Lock

SMS Kommando: eset lock <password>

Dieses Kommando sperrt das Gerät und verhindert somit den Zugriff für Unbefugte. Beim Sperren des Geräts per SMS erhält der Absender eine Antwort mit der IMEI- des Geräts und IMSI-Nummer der SIM Karte. Der Lock ist sehr robust gestaltet, wir konnten ihn nicht umgehen. Zudem ist das SMS Kennwort unterschiedlich zum Sperrpasswort. Ein Problem sehen wir nur beim Absetzen von Notrufen. Zwar ist ein Button „Emergency“ vorhanden, dieser hat aber keine Funktion. Entsperrt man dann das Gerät, so erscheint plötzlich der „Emergency Dialer“. Es scheint also so, als ob sich der Sperrbildschirm noch vor das Eingabefeld für Notrufnummern legen würde. ESET kündigte nach Rücksprache an dieses Problem für die nächste Version bereits behoben zu haben. ESET konnte das Problem auf ein kürzlich veröffentlichtes Sicherheitsupdate von Android zurückführen.

Siren

SMS Kommando: eset siren <password>

Dieses Kommando lässt eine sehr schrille Sirene ertönen und sperrt das Gerät gleichzeitig. Dies kann zum Beispiel beim Wiederfinden eines verlegten Geräts helfen oder einen Dieb dazu motivieren das Diebesgut loszuwerden.

Find

SMS Kommando: eset find <password>

Durch Absenden des Befehls per SMS wird an den Absender ein Link von Google Maps mit Koordinaten gesendet. Im Webinterface wird kontinuierlich geortet. Somit sind immer mehrere Standorte verfügbar und der Bewegungsverlauf des Geräts kann verfolgt werden.

Wipe

SMS Kommando: eset wipe <password>

Der Wipe löscht persönliche Daten vom Smartphone des Nutzers. Hierbei wird das Gerät nicht auf Werkseinstellungen zurückgesetzt sondern die Daten manuell gelöscht. Hierbei hat sich ESET auch viel Mühe gegeben und viele Kleinigkeiten, wie den Browserverlauf bedacht. Zurückgeblieben sind lediglich die SMS.

Sonstige Funktionen

Sollte das Gerät als gestohlen gemeldet sein, erstellt ESET automatisch Fotos mit der Frontkamera des Geräts. Diese sind

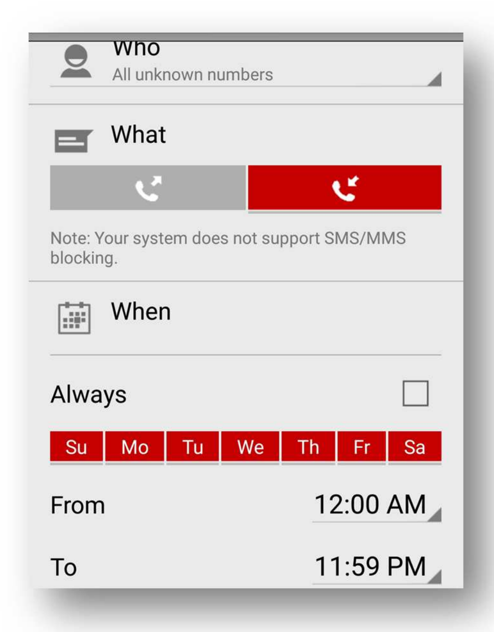


anschließend im Webinterface sichtbar. Somit lässt sich zum Beispiel ein Dieb identifizieren. Außerdem werden die Netzwerke erfasst, in welche sich das Gerät einbucht. Somit können Rückschlüsse gezogen werden, in welchem Umfeld sich das Gerät gerade aufhält.

Zusätzlich lassen sich alle erfassten Daten exportieren und als ZIP Datei herunterladen. Diese können dann etwa der Polizei übergeben werden um nach einem Dieb zu fahnden.

SMS & Call Filter

Diese Funktion bietet die Möglichkeit sehr umfangreiche Regeln zum Black- und Whitelisting von Anrufen und Nachrichten festzulegen. Es ist möglich eine Regel zu erstellen, die bestimmt was von welchen Nummern zu welchem Zeitpunkt geblockt oder durchgelassen werden soll. Es kann sowohl eine Regel für konkrete Nummern erstellt werden, als auch für unbekannte Anrufer, wie zum Beispiel solche mit versteckter Nummer.



In unserem Test zeigte uns ESET eine Meldung, dass das Blockieren von SMS mit dem System unseres Gerätes nicht funktioniert. Anrufe hingegen wurden wie erwartet abgewiesen.

Anti-Phishing

Anti-Phishing schützt den Benutzer beim Surfen im Internet vor Phishing. ESET überprüft alle installierten Browser auf Kompatibilität. ESET gibt an, dass diese Funktion nicht mit allen Browsern kompatibel ist, da nicht alle die erforderlichen Voraussetzungen erfüllen.

Der Phishingschutz hat in unserem Test mit Google Chrome einwandfrei funktioniert. Es erscheint eine Meldung, dass ESET empfiehlt die Seite unverzüglich zu verlassen.

Security Audit

Das Security Audit gibt Information über Systemeinstellungen und Programmrechte welche ein Sicherheitsrisiko darstellen können. Wir wurden in unserem Test unter anderem darauf aufmerksam gemacht, dass der USB-Debug-Modus sowie die Installation aus unbekannten Quellen aktiviert sind.

In einer Application Audit werden Apps in fünf Kategorien von möglichen Privatsphäreverletzungen eingeteilt. Die Kategorien sind Bezahldienste, Ortungsdienste, Abrufen der Identität, das Abrufen von Nachrichten sowie das Abrufen von Kontakten. Nähere Informationen zu Berechtigungen werden nicht geboten.

Updates

Die Virendefinition kann manuell aktualisiert werden. Zudem können Updates automatisch (zwischen sechs Stunden und zwei Wochen) ausgeführt werden.

Hilfe

Für jede Ansicht im Userinterface lässt sich durch ein Tippen auf das Fragezeichensymbol eine detaillierte Hilfe aufrufen. Diese beschreibt jeweils die aktuelle Ansicht und bietet ausreichende Detailtreue.

Deinstallation

Für die Deinstallation wird ein Assistent angeboten, welcher alle nötigen Schritte einleitet. Zuvor muss das Kennwort für den Diebstahlschutz eingegeben werden. Somit kann ein Dieb das Produkt nicht einfach Deinstallieren.



Lizenz

Eset Mobile Securtiy kann gratis aus dem Google Play Store bezogen werden. Um auf den vollen Funktionsumfang zugreifen zu können wird eine Premium Lizenz benötigt. Diese kann per In-App Einkauf für 9,99€ erworben werden.

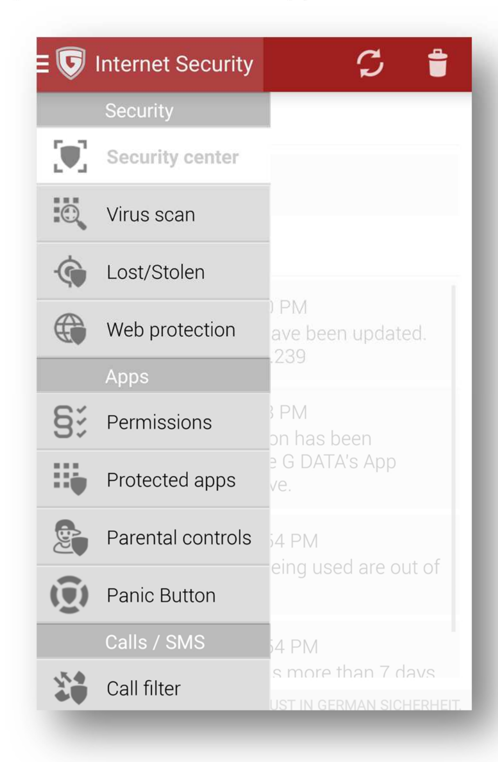
Fazit

ESET bietet ein umfangreiches Sicherheitsprodukt welches auch schon in der gratis Version, mit seinen sauber implementierten Funktionen, zu überzeugen weiß.



G Data Internet Security

G Data Internet Security ist ein sehr umfangreiches Sicherheitsprodukt welches neben den obligatorischen Komponenten wie Virenschutz und Diebstahlschutz auch noch Funktionen wie eine Kindersicherung und das Sperren von einzelnen Apps bietet.



Installation

G Data Internet Security wurde aus dem Google Play Store bezogen und installiert. Im ersten Schritt muss sich der Nutzer mit seinem G Data Account anmelden oder einen solchen registrieren. Letzteres initiiert eine 30 tägige Testversion der Premiumfunktionen. Anschließend wird der Diebstahlschutz konfiguriert. Hierfür muss ein mindestens vierstelliger PIN festgelegt werden. Außerdem wird die Telefonnummer einer Vertrauensperson abgefragt, welche etwa ein vergessenes Passwort zurücksetzen kann oder im Falle eines SIM-Kartenwechsels benachrichtigt wird. Anschließend wird G Data Internet Security optional als Geräteadministrator eingetragen um gegen unerlaubte Deinstallation zu schützen. Damit ist das Setup abgeschlossen.

Virus Scan

Die Virus Scan Komponente ermöglicht es dem Nutzer sein Smartphone auf Schadsoftware zu überprüfen. Hierbei kann er entweder nur die installierten Applikationen oder das gesamte System scannen. Die Resultate werden im Security Center angezeigt.

In den Einstellungen kann ein automatischer, zeitgesteuerter Scan aktiviert werden. Für die Frequenz kann 1, 3, 7, 14 oder 30 Tage gewählt werden. Gefallen hat uns, dass eingestellt werden kann, dass ein Scan nur bei ausreichend hohem Batteriestand durchgeführt wird. Außerdem kann festgelegt werden, dass der Scan nur während dem Aufladen des Smartphones stattfinden soll.

Lost/Stolen

Die Komponente ist nach der eingehenden Konfiguration bei der Installation bereits für die Nutzung über SMS konfiguriert. Der Nutzer muss nur noch die verschiedenen SMS Kommandos erlauben. Zusätzlich kann eine Verbindung mit dem Webinterface hergestellt werden. Da die Lizenzierung der App pro Gerät erfolgt muss die App hierfür einem unabhängigen Account hinzugefügt werden. Hierfür kann ein im Webinterface erzeugter QR-Code eingescannt werden. Danach ist die Anti-Theft Komponente auch über das Webinterface nutzbar. Weiters ist es möglich SMS vom Webinterface aus zu senden, was den Vorteil bringt, dass die Diebstahlschutzkomponente auch dann erreicht werden kann, wenn das Gerät über keine Internetverbindung verfügt, etwa im Ausland.

Lock

SMS Kommando: <Passwort> lock

Dieser Befehl sperrt das Gerät mittels des Android Lockscreen. Hierfür wird der auf dem Gerät eingestellte Lockscreen verwendet, ist keiner gesetzt wird ein PIN Lock mit dem festgelegten Passwort verwendet. Da das Passwort per SMS Kommando mitgesendet wird und SMS standartmäßig als Notifikation sichtbar sind kann das Passwort im letzten Fall



sehr einfach ausgelesen werden. G Data weist auf dieses Problem in seiner App nicht hin. Zusätzlich besteht beim verwendeten Android Lockscreen immer die Möglichkeit zum Gastnutzer zu wechseln.

G Data teilte uns nach Absprache mit, in der nächsten Version einen Warnhinweis einzuführen, der darauf aufmerksam macht, dass SMS im Sperrbildschirm angezeigt werden können, wenn nicht der Modus „Hide sensitive notification content" oder eine komplette Deaktivierung der Benachrichtigungen eingestellt wird. Zudem weist G Data darauf hin, dass der Nutzer darauf aufmerksam gemacht wird ungenutzte Benutzeraccounts zu deaktivieren, auch wenn wir dies auf der Android Version in unserem Test nicht möglich ist.

Wipe

SMS Kommando: <Passwort> wipe

Dieses Kommando setzt das Gerät auf Werkseinstellung und löscht somit alle Daten vom Gerät. Eine weitere Verwendung der Anti-Theft Komponente ist danach nicht mehr möglich.

Ring

SMS Kommando: <Passwort> ring

Dieses Kommando lässt ein Alarm auf dem Gerät ertönen. Das Gerät wird dabei nicht gesperrt.

Mute

SMS Kommando: <Passwort> mute

Dieses Kommando schaltet das Gerät stumm. Hierfür wird das Gerät in den Modus „Priorität" gesetzt.

Set Device Password

SMS Kommando: <Passwort> set device password <Geräte Passwort>

Setzt das für den Lockscreen zu verwendende Passwort. Wie bereits erwähnt ist auch diese SMS bei falscher Konfiguration sehr einfach auslesbar.

Remote Password reset

remote password reset: <neues Passwort>

Dieses Kommando ändert das zu verwendete Passwort für SMS Kommandos. Dies kann nur von der Vertrauenswürdigen Nummer aus gesendet werden.

SIM Change

Es ist mögliche beim Wechseln der SIM Karte eine Ortung und/oder eine Sperrung des Gerätes auszulösen. Es erfolgt zusätzlich eine Verständigung per E-Mail sowie per SMS an die vertrauenswürdige Nummer.

Locate on low Battery

Zusätzlich ist es möglich dass eine E-Mail und SMS mit dem aktuellen Standort des Gerätes versandt wird wenn das Gerät einen bestimmten Akkustand erreicht.

Web protection

Die Web Protection Komponente schützt den Nutzer während dem Surfen im Internet mit dem Android und Chrome Browser. In den Einstellungen kann festgelegt werden, dass die Web protection nur bei aktiver WLAN Verbindung tätig sein soll.



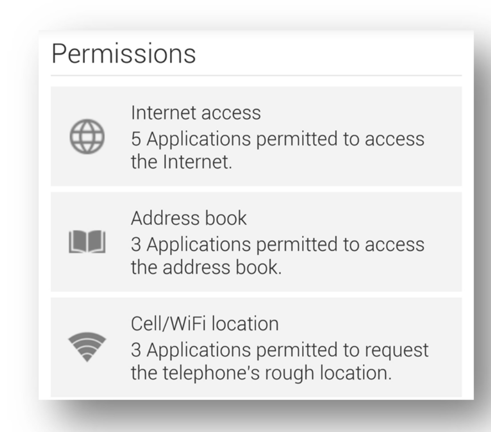
In unserem Kurztest hat diese Komponente gut funktioniert.

Permissions

Die Permissions Komponente zeigt installierte Applikationen auf, welche besondere Berechtigungen erfordern. Alle installierten Apps werden in Kategorien eingeteilt, wie zum Beispiel „Zugriff auf das Internet" oder „Berechtigung zur Ortung".



Durch Antippen einer dieser Einträge werden die entsprechenden Applikationen aufgelistet. Durch Antippen einer App, werden Details zu den Berechtigungen angezeigt, was unserer Ansicht nach sehr übersichtlich gestaltet wurde. Die Applikation kann aus dieser Ansicht direkt deinstalliert, oder zur „App protection" hinzugefügt werden.



Protected Apps

Die App Protection schützt Applikationen vor unbefugtem Zugriff. Es kann ein PIN festgelegt werden, welcher für die Ausführung ausgewählter Apps eingegeben werden muss. Auf unseren Kritikpunkt vom letztjährigen Report ist G Data nicht eingegangen. Nach wie vor kann der PIN durch die „Forgot password" Funktion an die Emailadresse des Nutzers geschickt werden. Diese ist meist mit dem Email App auf dem Gerät verknüpft, ein Unbefugter könnte über diesen Weg an den PIN gelangen. G Data könnte diesen Zustand leicht beheben, indem man die E-Mail App zu den empfohlenen Apps bei der App Protection hinzufügen würde, wo im Übrigen auch bereits andere Apps, wie die Einstellungen, angeführt sind. Auch hier ging G Data auf unseren Vorschlag zur Verbesserung ein und kündigte die Änderung mit nächster Version an. Ansonsten hat die Komponente aber verlässlich funktioniert.

Parental Controls

Diese Komponente wurde eingeführt um Kinder vor unangemessenen Inhalten zu schützen.

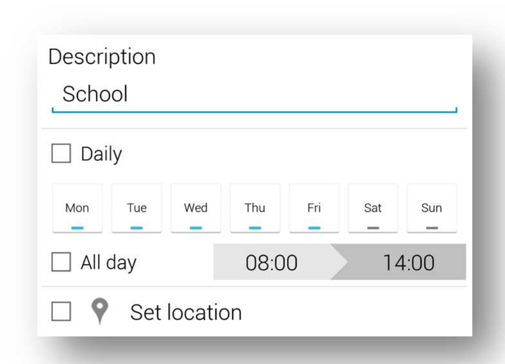
Beim Setup muss das Security Produkt statt des originalen Launchers jenen von G Data verwendet werden. Dieser legt sich vor die Oberfläche von Android und blendet alle installierten Applikationen aus. Es ist lediglich möglich jene Apps auszuführen, welche von den Eltern als sicher eingestuft werden. Im Zuge dessen kann auch die maximale Zeitspanne eingestellt werden, die das Kind gewisse Apps pro Tag nutzen darf. Um den Modus wieder zu verlassen ist ein PIN erforderlich.



In unserem Test hat die Komponente gut funktioniert. Einziger Schönheitsfehler war, dass es möglich war zu den zuletzt geöffneten Applikationen zu wechseln und diese durchzublättern. Das Öffnen nicht erlaubter Applikationen war uns nicht möglich insofern handelt es sich hierbei nicht um einen schwerwiegenden Fehler.

In einem eigenen Teenager Corner wird mehr auf die Bedürfnisse von Jugendlichen eingegangen. Es ist möglich die Nutzung des Geräts zeitlich zu limitieren. Zudem kann der Ort für die Regel bestimmt werden. Ein Beispiel hierfür wäre, dass die Nutzung werktags am Vormittag in der Nähe der Schule untersagt sein soll. Dies hat in unserem Test verlässlich funktioniert.





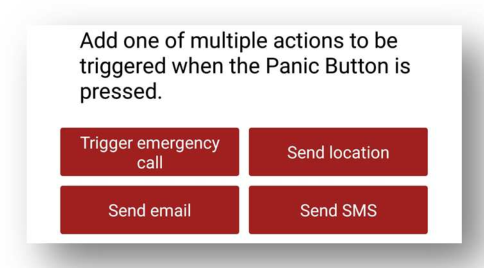
Ein Problem, das G Data sowohl mit dem Childern's, als auch mit dem Teenager Corner hat ist, dass es jeweils möglich ist die Notification Leiste nach unten zu ziehen und zur Benutzerverwaltung zu wechseln. Hier ist es möglich zu einem Gastkonto zu wechseln wodurch sich das Gerät praktisch uneingeschränkt nutzen lässt. G Data hat uns mitgeteilt, dass das Problem mittlerweile behoben wurde und die Korrektur in der nächsten Version integriert sein wird.

Kid's Browser

Der Kids Browser ist ein separates App, welches es speziell Kindern ermöglicht sicher Inhalte im Internet zu konsumieren. Für Eltern ist es möglich zu konfigurieren, ob die kinderfreundliche Suchmaschine http://fragfinn.de eingesetzt werden soll. Zudem ist es möglich über Listen Webseiten explizit zuzulassen oder auszuschließen.

Panic button

Der Panic Button ist eine Funktion, die es ermöglicht ein Widget auf dem Startbildschirm zu platzieren. Tippt der Nutzer in einem Notfall auf dieses wird eine zuvor definierte Aktion (Notruf, Senden der Position, Senden einer Email, Senden einer SMS) ausgeführt.

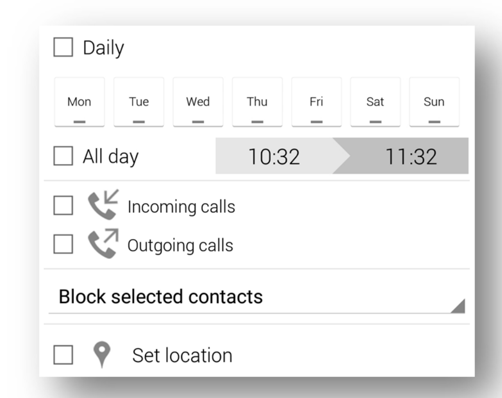


Call Filter

Dieser Teil der Applikation ermöglicht das Blockieren von unerwünschten Anrufen und SMS. Es ist möglich Regeln für die Blockierung eingehender Anrufe und SMS zu erstellen, sowie für ausgehende Anrufe.

Es kann entweder Black- oder Whitelisting eingestellt werden. Beim Blacklisting kann der Nutzer angeben, welche Nummern blockiert werden sollen. Alle anderen werden durchgelassen. Zusätzlich kann eingestellt werden, ob die Kontakte aus der Kontaktliste immer zugelassen werden sollen. Mit einer Checkbox kann der Nutzer entscheiden, ob unbekannte Nummern zugelassen werden sollen, oder nicht.

In unseren Tests hat diese Funktion verlässlich funktioniert. Nur das Blockieren von SMS hat nicht geklappt. Dies liegt vermutlich an der verwendeten Android Version unseres Testgeräts. G Data macht jedoch nicht darauf aufmerksam, dass diese Funktion mit der Android Version nicht kompatibel ist.



Hide Contacts

Die Hide Contacts Komponente von G Data kann die Kommunikation mit bestimmten Kontakten, sowie die Kontakte selbst verstecken. Hierfür wird ein eigener Messenger geboten, welcher das Senden und Empfangen von SMS Nachrichten übernimmt.

In unserem Test hat diese Komponente nicht funktioniert. Sowohl ausgehende, als auch



eingehende Nachrichten wurden angezeigt. Wir führen auch dies auf eine inkompatible Android Version zurück. G Data macht auch auf diesen Missstand nicht aufmerksam. G Data stimmte auch hier zu in der nächsten Version eine Warnung einzublenden. Zudem informierte uns G Data, dass eine eigene SMS Komponente verfügbar sei, welche auf jeder Android Version kompatibel ist. Hierfür muss die App als Standardapp für den SMS Empfang eingerichtet werden. Das Verstecken des Anrufverlaufes hat einwandfrei funktioniert.

Updates

Updates werden automatisch in definierbaren Intervallen (alle 1, 3, 7, 14 oder 30 Tage) durchgeführt. Es kann eingestellt werden ob Updates nur über WLAN oder auch das Mobilfunknetz bezogen werden sollen.

Hilfe

Bei einfachen Komponenten ist direkt eine einfache Erklärung zur Funktionsweise vorhanden, bei komplexeren Komponenten wird oben rechts eine Fragezeichen eingeblendet welches zu einer ausführlichen Hilfe führt.

Deinstallation

Wenn der Deinstallationsschutz aktiviert ist muss zuerst die App als Geräte Administrator deaktiviert werden. Hierfür wird das Passwort benötigt.

Lizenz

Eine Lizenz gibt es über den Play Store für €1,99 monatlich oder €18,99 jährlich. Über die Webseite von G Data kann eine Jahreslizenz für €15,95 erworben werden. In der „lite“ Version ist die Funktionalität auf den Virenschutz beschränkt.

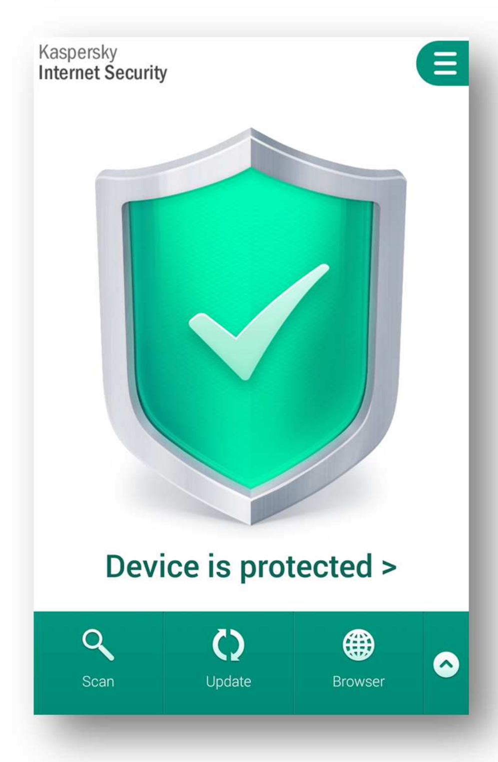
Fazit

Der Nutzer erhält mit G Data Internet Security ein umfangreiches Sicherheitsprodukt, welches bei der Verwendung der SMS Kommandos kleine Sicherheitsprobleme aufweist.



Kaspersky Internet Security

Kaspersky Internet Security ist eine umfangreiche Sicherheitsapp die sowohl als Free-, wie auch als Pro-Version erhältlich ist.

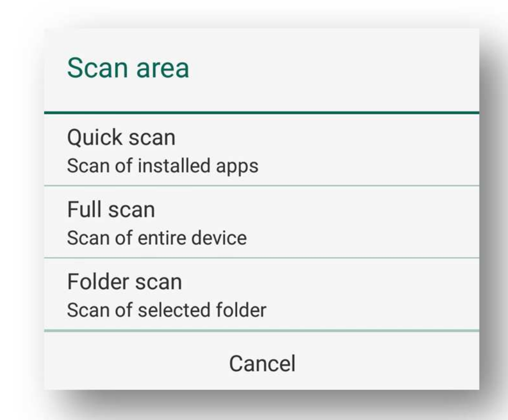


Installation

Kaspersky Internet Security wurde aus dem Google Play Store bezogen und installiert. Im ersten Schritt muss der Nutzer das Land, in dem er lebt, einstellen. Anschließend müssen die Lizenzvereinbarungen akzeptiert werden.

Scan

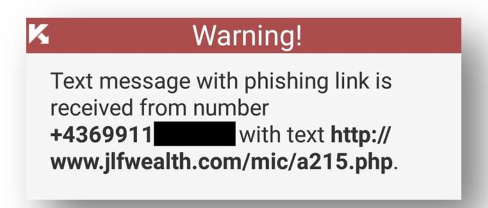
Diese Komponente von Kaspersky Internet Security ermöglicht es dem Nutzer das Gerät nach Schadsoftware zu scannen.



Hierfür werden drei unterschiedliche Modi angeboten: Quick Scan untersucht alle installierten Apps, Full Scan das ganze Gerät und mit einem Folder Scan können spezifische Ordner gescannt werden. In den Einstellungen kann der Nutzer entscheiden ob die Cloud für die Erkennung verwendet werden soll. Zudem ist es möglich automatische Scans zu definieren (täglich, wöchentlich).

Browser

Kaspersky bietet für den Schutz des Users während des Surfens im Internet einen Browserschutz an. Kaspersky gibt an gegen Malware und Phishing Attacken zu schützen. Die Schutzfunktion ist nur mit dem Standardbrowser kompatibel. In unserem Kurztest hat diese Komponente einwandfrei gearbeitet.



Ein weiterer Bestandteil der Webprotection schützt den Nutzer vor Phishinglinks, welche per SMS an den Nutzer gesendet werden.

Privacy Protection

Beim Aktivieren dieser Funktion warnt Kaspersky wieder, dass es beim Empfangen und Senden von Nachrichten Probleme mit der Android Version 4.4 und höher geben kann.
Im folgenden Schritt muss der Nutzer eine Lizenzvereinbarung akzeptieren, die vor allem die Nutzung der Daten betrifft. Anschließend muss Kaspersky als Geräteadministrator eingetragen werden. Hier meldet die Applikation, dass sie gerne der einzige Geräteadministrator auf dem Gerät wäre. Somit wird gefordert, dass Google Play Services von den Geräteadminstratoren ausgetragen werden. Dieser Schritt kann jedoch auch übersprungen werden. Zudem muss sich der Nutzer mit seinem Kaspersky Account anmelden. Im Anschluss wird der Nutzer



aufgefordert einen Sicherheitscode zu definieren. Kaspersky empfiehlt diesen aufzuschreiben und sicher abzulegen.

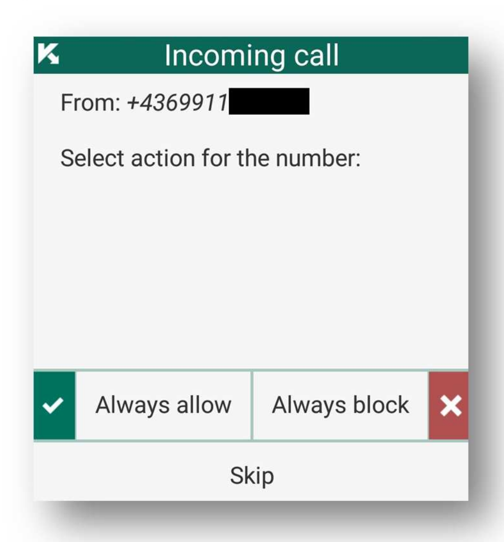
Nach der Aktivierung wird das Einstellungsmenü für Privacy Protection angezeigt. Dieses Modul erlaubt das Verstecken von Kontakten im Adressbuch, sowie SMS und Anruflogs. Die zu versteckenden Kontakte können über ein einfaches Menü definiert werden.

In unseren Tests hat diese Komponente insgesamt sehr gut funktioniert. Die Kontakte wurden ausgeblendet, ebenso wie die Anruflogs. Die SMS waren jedoch noch im Posteingang. Für das Deaktivieren der Privacy Protection ist die Eingabe eines PIN Codes erforderlich.

Call & Text Filter

Beim ersten Start der Komponente erscheint ein Popup, welches darauf hinweist, dass es aufgrund technischer Einschränkungen von Android Versionen größer gleich 4.4 zu Problemen beim Senden und Empfangen von Nachrichten kommen kann.

Anschließend wird ein schlicht gehaltener Dialog angezeigt. Mit Black- und Whitelists können Nummern entweder geblockt oder explizit erlaubt werden.

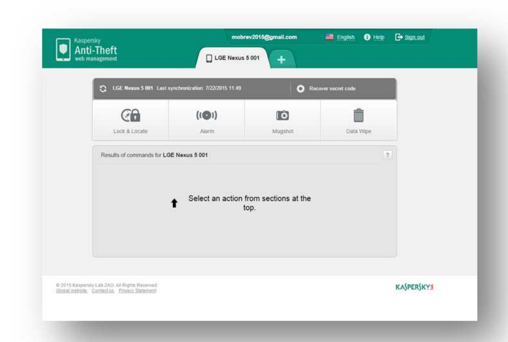


Kaspersky bietet verschiedene Modi für die Blockierung: *Blocked Contacts* blockiert alle Nummern, welche auf der Blacklist stehen. *Allowed Contacts* erlaubt nur SMS und Anrufe von Nummern, welche auf der Whitelist stehen, alle anderen werden abgewiesen. Im *Standard Modus* werden Nummern aus der Blacklist abgewiesen und Nummern aus der Whitelist zugelassen. Für solche, die auf keiner der beiden Listen stehen, wird eine Dialogbox angezeigt um den Nutzer entscheiden zu lassen, wie mit dem Anrufer weiter verfahren werden soll. Für die Blacklist kann bestimmt werden, ob nur SMS, nur Anrufe, oder beides abgewiesen werden sollen.

Das Blockieren der Telefonanrufe hat in unserem Test gut funktioniert. SMS wurden aufgrund von Limitierungen in Android nicht geblockt, wie auch schon von Kaspersky angekündigt.

Anti-Theft

Der Diebstahlschutz von Kaspersky wird über ein Webinterface (http://anti-theft.kaspersky.com) gesteuert. Zusätzlich sind SMS Kommandos verfügbar.



Lock and Locate

SMS Kommando: Find: <PIN>

Diese Funktion ermöglicht das Orten und Sperren des Geräts. Nach der Ortung wird die Position in einer Google Maps Karte eingetragen. Gleichzeitig wird das Gerät mit dem Android internen Sperrbildschirm gesperrt. Dieser ist im Allgemeinen sehr sicher und wir konnten ihn nicht umgehen. Sollte der Nutzer den PIN vergessen haben, so kann er



einen Recovery Code im Webinterface abrufen. Dieser ist 16 Stellen lang und lässt anschließend den orginalen PIN im Klartext erscheinen. Gut gefallen hat uns auch, dass es möglich ist eine personalisierte Nachricht am Sperrbildschirm anzeigen zu lassen. Hier könnten etwa Kontaktinformationen eingetragen werden.

Bei der Verwendung von SMS Kommandos erhält der Absender ein SMS mit den Koordinaten des Geräts. Dies ist jedoch sehr unhandlich. Hier wäre es wohl sinnvoller direkt Links zu Kartendiensten zu versenden. Außerdem war es uns möglich eingegangene SMS auf dem Sperrbildschirm anzuzeigen (betrifft Android 4.4 und höher). Dies hat zur Folge, dass ein Dieb den PIN zum Entsperren sehr leicht herausfinden und das Gerät entsperren kann. Dramatisch wäre dies nicht, wenn man für den Sperrbildschirm einen anderen PIN oder ein Lock-Pattern vergeben könnte. Kaspersky überschreibt bestehende Sicherheitsfeatures jedoch einfach wodurch ein Zugriff auf das Gerät kinderleicht wird. Abhelfen kann sich ein Nutzer nur indem er in den Einstellungen sämtliche Notifications auf dem Sperrbildschirm deaktiviert. Auf diesen Zustand macht Kaspersky jedoch nicht aufmerksam.

Alarm

SMS Kommando: Alarm: <PIN>

Diese Funktion sperrt das Gerät und lässt einen Alarmton ertönen. Dies kann beim Wiederfinden eines verlegten Geräts hilfreich sein.

Mugshot

Diese Funktion erstellt Fotos des Diebs mit der Frontkamera. Diese werden anschließend im Webinterface der Diebstahlsicherung angezeigt was helfen kann einen Dieb zu identifizieren. Dieses Kommando ist nur für das Webinterface verfügbar, nicht für SMS.

Wipe

SMS Kommando: Wipe: <PIN>

Die Wipe Funktion löscht persönliche Daten vom Gerät des Nutzers. So kann verhindert werden, dass möglicherweise vertrauliche Informationen in die Hände Unbefugter gelangen.

Kaspersky bietet zwei unterschiedliche Arten von Wipes an. Bei der ersten Variante werden nur die persönlichen Daten vom Gerät gelöscht. Dazu gehören Kontakte, Nachrichten, Kalender und Google Account. Der Diebstahlschutz bleibt hierbei aktiv. In unseren Tests wurden alle Daten gelöscht, jedoch nicht der Browserverlauf und die Favoriten.

Bei der zweiten Variante wird das Gerät zusätzlich aus Werkseinstellungen zurückgesetzt (***SMS Kommando: fullreset: <PIN>)***. In diesem Fall wurden alle Daten gelöscht, jedoch ist in diesem Fall der Diebstahlschutz nicht mehr aktiv.

SIM Watch

Die SIM Watch Funktion erkennt, wenn eine andere SIM Karte eingelegt wurde, zum Beispiel die eine Diebes. In diesem Fall wird das Gerät gesperrt. Zusätzlich kann eine Nummer und eine Emailadresse eingetragen werden, welche im Falle eines SIM Wechsels kontaktiert wird.
Die Funktion hat in unserem Test sehr gut funktioniert. Das Gerät wurde gesperrt, Benachrichtigungen per SMS und Email wurden versandt.

Updates

Updates werden automatisch ausgeführt (Einstellbar täglich oder wöchentlich). Zudem können Aktualisierungen manuell angestoßen werden.

Hilfe

Kaspersky bietet eine wirklich umfangreiche Hilfe an. Diese sollte ausreichend Informationen bieten um etwaige Probleme zu lösen. In den meisten Dialogen ist in der rechten oberen Ecke eine sehr kleine Fragezeichenbox, welche den Nutzer direkt zu der entsprechenden Hilfeseite leitet.



Deinstallation

Ist die App als Geräteadministrator eingetragen muss dies zuerst deaktiviert werden. Danach kann die App ohne Passwortabfrage deinstalliert werden. Die neuere Version (11.9) bietet eine optionale Passwortabfrage vor der Deinstallation.

Lizenz

Kaspersky Mobile Security ist als Free Version mit eingeschränktem Funktionsumfang erhältlich. Für etwa 10,95€ kann man die Jahreslizenz für die Pro Version in Europa erwerben. Diese bietet die zusätzlichen Funktionen Real-time, Web und Privacy Protection sowie Phishing Schutz über SMS.

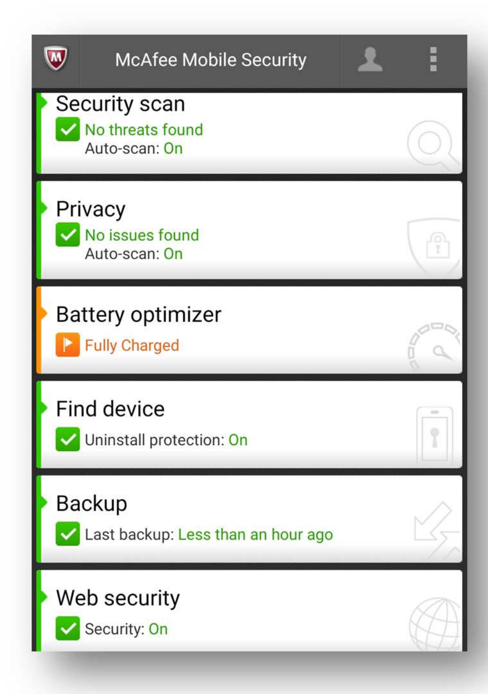
Fazit

Kaspersky bietet ein umfangreiches Sicherheitsprodukt welches auch in der Free Version die wichtigsten Funktionen unterstützt. Die Premiumversion beinhaltet unter anderem eine Privacy protection und einen Phishing Schutz für SMS Nachrichten, welcher in unserem Test gut funktionierte. Wie auch bei anderen Produkten anderer Hersteller gibt es auch hier Limitierungen aufgrund der im Test verwendeten Android Version.



McAfee Mobile Security

McAfee Mobile Security bietet neben Malware- und Diebstahlschutz unter anderem noch eine Privacy Control Komponente welche Funktionen wie Benutzerprofile und Anruffilter beinhaltet. Auch eine Backup-Funktion ist vorhanden welche es dem Nutzer ermöglicht automatisiert oder aus dem Webinterface heraus ein Backup anzustoßen.



Installation

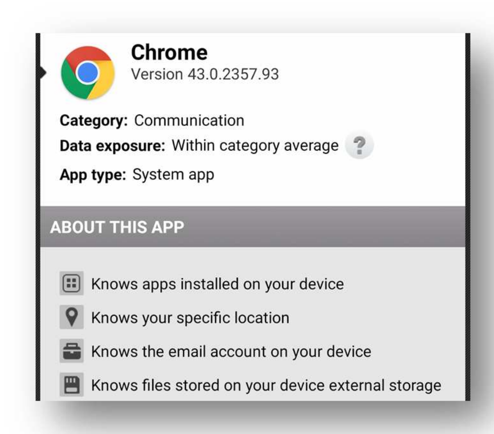
McAfee Mobile Security wurde aus dem Google Play Store bezogen und installiert. Im ersten Schritt müssen die Lizenzbedingungen akzeptiert werden. Anschließend ist das Setup beendet.

Security Scan

Diese Komponente erlaubt es dem Nutzer sein Smartphone auf Schadsoftware zu überprüfen. Der Scan kann auch zeitgesteuert automatisch gestartet werden. Hierfür können die Intervalle „täglich" und „wöchentlich" gewählt werden. In den Optionen kann der Nutzer den Umfang eines Scans einstellen. So kann entschieden werden ob installierte Apps untersucht werden sollen. Zudem kann eingestellt werden ob PUA in die Erkennung miteinbezogen und ob Dateien untersucht werden sollen.

App Privacy

Die App Privacy Funktion erlaubt es dem Nutzer installierte Applikationen auf mögliche Verletzungen der Privatsphäre zu prüfen. Alle Apps werden in einer List angeführt und in verschiedene Gefahrenklassen eingeteilt. In unserem Test waren nur „Medium" und „Low" vorhanden. Schwerwiegende Fälle von Verletzungen werden in eine eigene Liste „Privacy Alerts" eigetragen.



Durch Antippen werden Details zur App gegeben und Gründe für die Beanstandung angeführt, wie zum Beispiel, dass die Applikation die Möglichkeit besitzt das Gerät zu orten. In den Einstellungen kann aktiviert werden, ob Privacy Scans automatisch täglich oder wöchentlich durchgeführt werden sollen.

Privacy Control

Die Privacy Control ermöglicht es dem Nutzer persönliche Daten zu schützen, sowie Störenfriede abzuweisen. Nachfolgende Funktionen werden hierfür angeboten.

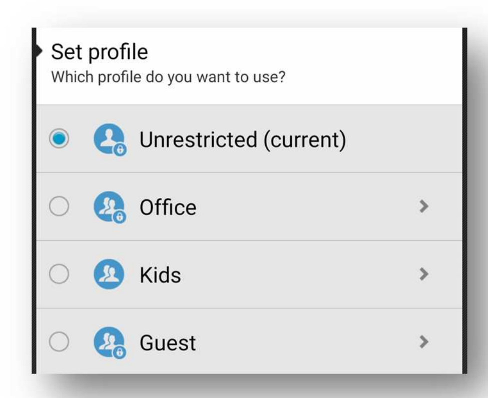
Lock Apps

Die Lock Apps Funktion ermöglicht es dem Nutzer installiere Applikationen mit einem PIN zu sperren. Dieser muss vor dem Start einer App eingegeben werden. In der Konfiguration kann der Nutzer aus einer Liste aller Anwendungen auswählen welche geschützt werden sollen. In unseren Tests funktionierte der App Lock wie erwartet. Es war uns nicht möglich eine gesperrte Applikation ohne PIN zu verwenden.



Set Profile

McAfee Mobile Security ermöglicht es dem Nutzer aus einem von vier Profilen zu wählen (Keine Einschränkung, Büro, Kinder, Gast). Für jedes dieser Profile kann gewählt werden, welche Applikationen verfügbar sein sollen. Um andere Apps auszuschließen hat McAfee einen eigenen Launcher implementiert, welcher nur die erlaubten Apps anzeigt.



Beim Versuch zum originalen Startbildschirm zurückzuwechseln um Zugriff auf alle installierten Apps zu erhalten ist die Eingabe des Pins erforderlich.

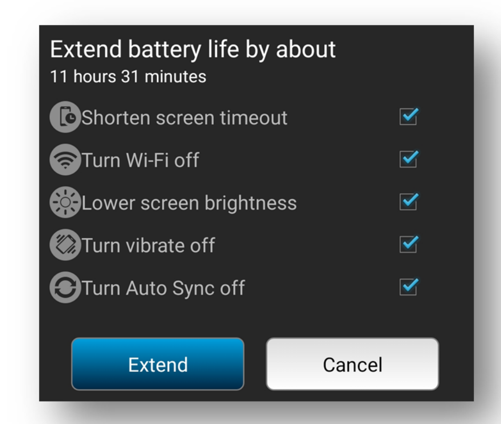
In unseren Tests war es uns möglich durch das Öffnen der Notification Bar zu einem Gastprofil zu wechseln. Dort könne allerdings nur vorinstallierte Apps, wie etwa der Chrome Browser, verwendet werden. Dies gilt auch dann, wenn es eigentlich durch McAfee verboten sein sollte. Mcafee erklärte uns, dass dieses Verhalten nur bei Smartphones mit Vanilla Google Stock Images (wie Nexus oder Moto G auftritt). Bei anderen Geräten funktioniere die Funktion wie erwartet.

Block Calls

Um unerwünschte Anrufe abzuweisen liefert McAfee die Funktion „Block Calls“ mit. Diese arbeitet sowohl mit Black- als auch mit Whitelists. In den Einstellungen kann festgelegt werden wie die Filterfunktion für eigehende-, ausgehende- und Roaminganrufe arbeiten soll. Für jede der drei Arten kann der Nutzer definieren ob alle erlaubt, nur Anrufe aus der Whitelist erlaubt, Anrufe aus der Blacklist blockiert, oder überhaupt alle Anrufe blockiert werden sollen. Zusätzlich kann der Nutzer entscheiden ob Anrufer mit unterdrückter Nummer blockiert werden sollen, oder nicht. Die Block Calls Komponente hat in unseren Tests verlässlich funktioniert.

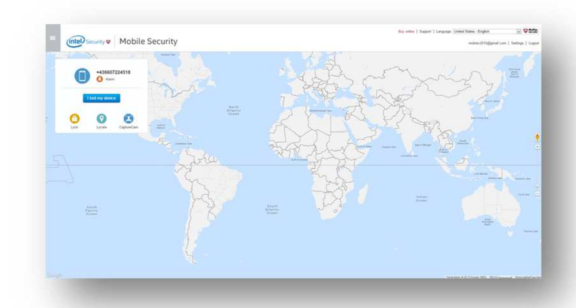
Battery Optimizer

Der Battery Optimizer ermöglicht laut Angaben des Herstellers die Verbesserung der Akkulaufzeit, sowie der Leistung des Geräts. Durch Tippen des Extend Battery Buttons können automatisch Einstellungen zur Verlängerung der Akkulaufzeit vorgenommen werden, etwa durch Verringerung der Displayhelligkeit. Zudem kann ein Memory Cleaner den Speicher von aktiven Apps bereinigen.



Find Device

Unter dem Menüpunkt „Find Device“ findet der Nutzer den Diebstahlschutz. Dieser wird entweder über ein Webinterface (https://www.mcafeemobilesecurity.com) oder über SMS Kommandos gesteuert.





Orten

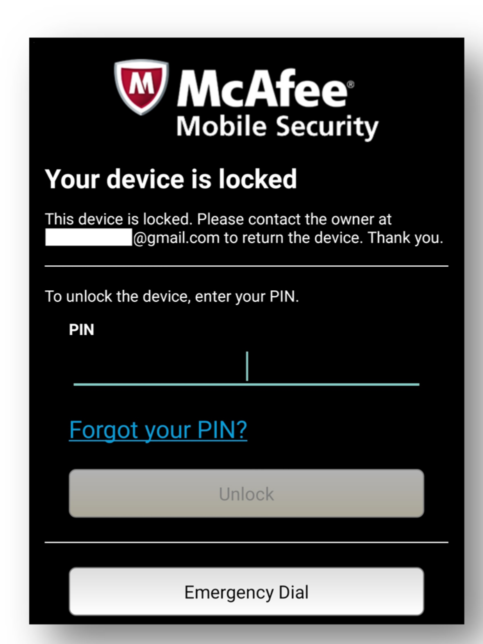
SMS Kommando: Secure locate <PIN>

Diese Funktion ortet ein verlorengegangenes oder gestohlenes Gerät. Anschließend wird die Position in einer Karte von Google Maps dargestellt. Im Falle einer Ortung per SMS wird dem Sender des Befehls ein Link auf eine Webseite von McAfee gesendet, wo eine Google Maps Karte eingebettet ist. Gefallen hat uns, dass es möglich ist den Bewegungsverlauf des Geräts aufzunehmen. McAfee Warnt jedoch davor, dass dies die Batterie stark belastet.

Sperren

SMS Kommando: Secure lock <PIN>

Diese Funktion sperrt das Gerät aus der Ferne und verhindert somit den Zugriff von Unbefugten. Die Sperren-Funktion kann mit der Alarm-Funktion kombiniert werden, welche im folgenden Abschnitt näher erklärt wird.



In unserem Test hat diese Funktion ausgesprochen gut funktioniert. Es war uns nicht möglich auf den Homescreen, die Notification Bar oder andere Ansichten zuzugreifen. Außerdem war es zu jeder Zeit möglich einen Notruf abzusetzen. Es ist möglich eine Nachricht für den Sperrbildschirm zu definieren.

CaptureCam

SMS Kommando: Secure message <PIN>

Die CaptureCam nimmt mit der Frontkamera des Smartphones ein Foto auf, welches dem Nutzer anschließend per Mail zugesandt wird. So kann er feststellen wer gerade das Gerät in Verwendung hat. McAfee hat eine raffinierte Methode entwickelt, die sicherstellt, dass das Gesicht des Diebs fotografiert wird und nicht etwa die Innenseite der Hosentasche.

Die Basisfunktionalität ist zufriedenstellend, jedoch verstehen wir nicht, warum die aufgenommenen Fotos nicht im Webinterface eingesehen werden können, wie jeglicher andere Content auch. Gefallen hat uns hingegen, dass bei mehrmaliger Falscheingabe des PINs automatisch ein Foto mit der Frontkamera erstellt wird.

Alarm

SMS Kommando: Secure alarm <PIN>

Dieses Kommando bewirkt das Ertönen eines Signaltones. Dies kann dem Wiederfinden eines verlorenen Smartphones dienen. Außerdem kann die Funktion in Kombination mit der Sperren-Funktion eventuell einen Dieb dazu bewegen das Gerät liegen zu lassen.

Löchen

SMS Kommando: Secure wipe <PIN>

Dieser Befehl löscht persönliche Daten des Nutzers vom Smartphone. Hierbei wird das Gerät nicht auf Werkseinstellungen zurückgesetzt, was den Vorteil bringt, dass der Diebstahlschutz weiterhin aktiv bleibt. In unserem Test wurden hier lediglich Kontakte, Telefonlog und der interne Speicher gelöscht. Vergessen wurde das Abmelden des Google-Accounts was auch die damit verbundenen Email und Kalender Apps betrifft. Auch die Browserdaten Lesezeichen und Verlauf wurden in unserem Test nicht gelöscht. Da eine Löschung aber nur nach einer Sperrung des Gerätes erfolgen kann ist es ohnehin nicht möglich an diese Daten zu kommen.

Auf Werkseinstellungen zurücksetzen

SMS Kommando: Secure reset <PIN>

Mit diesem Kommando wird das Gerät auf Werkseinstellungen zurückgesetzt. Danach



kann der Diebstahlschutz aufgrund des Resets nicht mehr verwendet werden. Diese Funktion sollte erst dann eingesetzt werden, wenn auf ein Wiedererlangen des Geräts nicht mehr zu hoffen ist.

SIM-Karte überwachen

Dieses Feature sperrt das Gerät wenn eine fremde SIM Karte eingelegt wurde. Der User wird zusätzlich per Email über den Wechsel benachrichtigt.

Backup

Für den Fall, dass das Gerät des Nutzers entweder verlorengegangen oder kaputt ist hat McAfee eine Backupfunktion implementiert. Diese ermöglicht die Sicherung von Textnachrichten, Anruflogs, Kontakten sowie Mediendateien wie Videos und Bilder auf Server von McAfee. Diese sind anschließend im Webinterface sichtbar und downloadbar. Backups können entweder manuell angestoßen oder von McAfee automatisch durchgeführt werden. Hierfür lässt sich kein Intervall definieren, jedoch kann eingestellt werden, dass die Synchronisation nur über WiFi erfolgen darf. Außerdem lässt sich die Sicherung aus dem Webinterface heraus für Kontakte, SMS und Anruflogs anstoßen. Dies kann sinnvoll sein, wenn das Gerät verloren wurde. In einem derartigen Fall kann der Nutzer wenigstens noch seine Daten sichern.

Eine weitere Funktion der Backupkomponente ist das sichere Löschen von Daten auf dem Smartphone. Es können Kontakte, Anruflogs, die SD Karte, Photos und Videos gelöscht werden. Dies kann zum Beispiel sinnvoll sein, wenn der Nutzer sein Gerät verkaufen möchte und zuvor das Gerät von persönlichen Daten bereinigen möchte.

Web Security

Die Web Security schützt den Nutzer während dem Surfen im Internet vor schadhaften Webseiten. Dies hat in unserem Kurztest auch verlässlich funktioniert. Zusätzlich bietet McAfee eine Wi-Fi Security. Diese warnt den Nutzer, wenn sich dieser mit einem unsicheren WLAN-Netzwerk verbindet.

Updates

Updates werden automatisch täglich oder wöchentlich durchgeführt. Zusätzlich können Aktualisierungen manuell angestoßen werden.

Hilfe

Das App bietet sowohl Tutorials als auch Hilfeseiten.

Deinstallation

Für die Deinstallation muss der PIN eingegeben werden.

Lizenz

McAfee ist gratis aus dem Play Store installierbar es kann aber auf eine Bezahlte werbefreie premium Version gewechselt werden. Diese beinhaltet unter anderem 2Gb Onlinespeicher um ein Backup für Medien Dateien ausführen zu können.

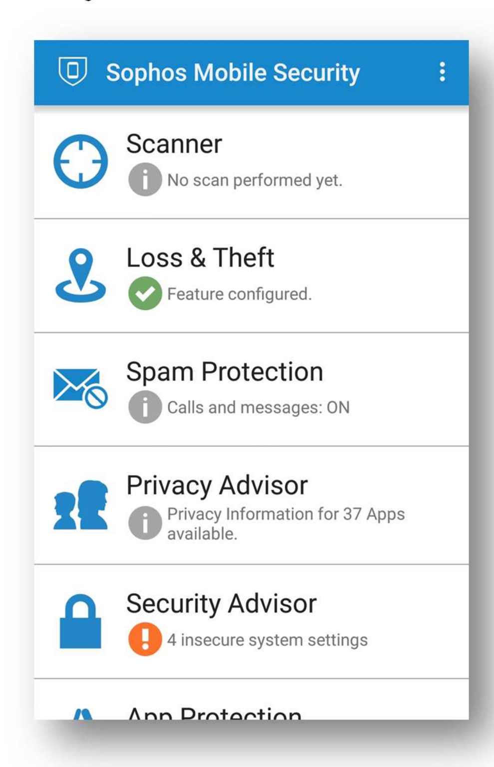
Fazit

Mit McAfee Mobile Security erhält man eine durchdachte Sicherheitsapp mit vielen nützlichen Funktionen. In unseren Tests machte die App einen stabilen Eindruck und auch die Diebstahlschutz Komponente funktionierte zu verlässlich.



Sophos Mobile Security

Sophos Mobile Security ist eine umfangreiche App die neben klassischen Malwarescanns zusätzlich auch noch aktiv mit der Komponente Web Filtering vor Gefahren wie z.B. Phishing schützen kann. Neben der SMS gesteuerten Loss & Theft Komponente bietet Sophos noch das Filtern von Anrufen und SMS, das Sperren von Apps sowie einen Privacy- und einen Security-Advisor.



Installation

Sophos Mobile Security wurde aus dem Google Play Store bezogen und installiert. Nach dem Akzeptieren der EULA kann der Nutzer entscheiden ob er anonyme Statistiken an Sophos senden möchte. Danach ist das Setup abgeschlossen.

Scanner

Die Scanner Komponente erlaubt das Überprüfen des Smartphones auf Malware. Hierfür wird dem Nutzer eine Vielzahl an Einstellungsmöglichkeiten geboten. Wie z.B. die Aktivierung des Cloudscans oder das Scannen von Systemapps und der SD-Karte. Zudem kann definiert werden ob bei der Live Protection auf PUA untersucht werden soll und ob ein Monitor für die SD Karte aktiviert werden soll. Zudem ist es möglich Scans in definierten Zeitabständen automatisch durchführen zu lassen. So kann eingestellt werden, dass alle 6 Stunden, 12 Stunden, täglich, alle zwei oder alle drei Tage automatisch ein Scan durchgeführt werden soll.

Loss & Theft

Mit dieser Komponente ist es möglich einen Alarm abzuspielen, das Gerät zu sperren, zu orten oder darauf befindliche Daten zu löschen. Dies geschieht durch Senden von SMS Nachrichten. Ein Webinterface wird nicht angeboten. Akzeptiert werden die Befehle jeweils nur von vertrauenswürdigen Nummern, die im Vorfeld definiert werden müssen. Zusätzlich benötigt der Sender ein Passwort um die Kommandos versenden zu können. Kommandos von anderen Nummern werden, selbst mit gültigem Passwort, ignoriert. Gefallen hat uns, dass beim Starten der Diebstahlschutzkomponente eine schöne Übersicht geboten wird, die signalisiert welche der Komponenten aktiv sind, und welche noch einer weiteren Konfiguration bedürfen.

Durch Einschränkungen von Android ab Version 4.4 können SMS nicht mehr versteckt werden. Dies hat zur Folge, dass nach dem Absetzen eines SMS Kommandos das Passwort auf dem Bildschirm sichtbar ist. Zwar hat dies keine direkte sicherheitstechnische Relevanz, da für das Entsperren die zuvor definierte Authentifizierung von Android verwendet wird, jedoch sollte der Nutzer trotzdem aufmerksam sein und auf keinen Fall dasselbe Kennwort bei anderen Diensten nutzen.

Alarm

SMS Kommando: alarm <Passwort>

Lässt für eine Minute einen Alarm ertönen. Das Gerät wird währenddessen gesperrt.

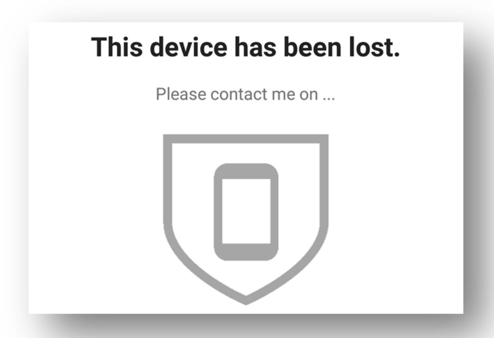
Lock

SMS Kommando: lock <Passwort>[<Nachricht>]

Das Gerät wird mit dem Android Sperrbildschirm gesperrt, welcher im



Allgemeinen nicht umgangen werden kann. Es kann eine Nachricht auf dem Bildschirm angezeigt werden, um einem Finder Kontaktmöglichkeiten anzuzeigen. Die anzuzeigende Nachricht kann frei gewählt werden indem der Nutzer die entsprechende Zeichenfolge an das SMS Kommando anhängt.



In unserem Test konnten wir feststellen, dass es möglich war über die Notification Leiste zu einem Gastkonto zu wechseln. Dies ist auf die verwendete Android Version zurückzuführen und kann nicht von Sophos beeinflusst werden. Demnach ist es einem Dieb möglich einen Teil der Funktionen zu verwenden, auch wenn er das Passwort nicht kennt.

Locate

locate <Passwort>

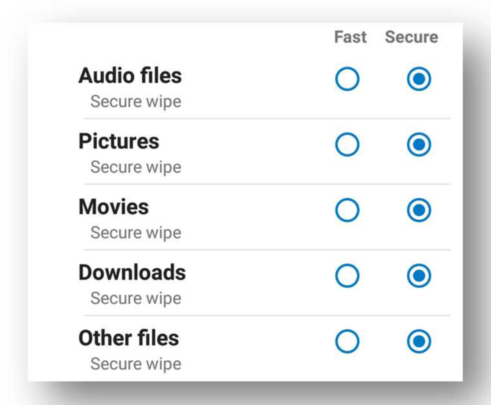
Nach dem Absetzen des Kommandos versucht das Telefon mittels GPS und WiFi seine Position zu bestimmen. Nach erfolgreicher Lokalisierung erhält der Sender eine Nachricht mit den Koordinaten und einem Link auf Google Maps. Der Benutzer erhält diese Nachricht zuerst mit einer ungefähren Position und nach einiger Zeit mit einer genaueren. Zudem kann eingestellt werden, dass die Position immer dann an die vertrauenswürdige Nummer geschickt wird, wenn das Gerät wenig Akku hat.

Sim Change

Da Sophos den Nutzer zwingt einen Sperrbildschirm einzusetzen ist das Gerät nach dem Einschalten automatisch gesperrt. Eine vertrauenswürdige Nummer wird entsprechend per SMS verständigt.

Wipe

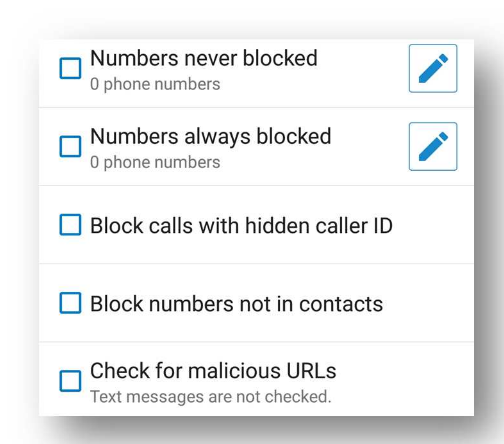
Die Wipe Funktion löscht persönliche Daten vom Gerät des Nutzers. Für das Löschen der SD-Karte bietet Sophos ein optionales sicheres Löschen an, hierbei werden die gelöschten Daten zusätzlich überschrieben. Diese Einstellung kann für einzelne Dateikategorien getrennt getroffen werden. Anschließend wird in beiden Fällen das Gerät auf Werkseinstellungen zurückgesetzt.



Spam Protection

Die Spam Protection schützt den Nutzer vor unerwünschten Anrufen und SMS. Obwohl die Schutzfunktionen jeweils global ein- und ausgeschalten werden können, ist dies für einzelne Nummern nicht möglich, so ist es z.B. nicht möglich nur die SMS Nachrichten einer Nummer zu blockieren. Sophos wird über ein Regelset konfiguriert, welches von oben nach unten abgearbeitet wird. Es ist möglich Nummern explizit zuzulassen, zu blockieren und unterdrückte oder unbekannte Nummern abzuweisen. Zudem können SMS auf schadhafte URLs überprüft werden.

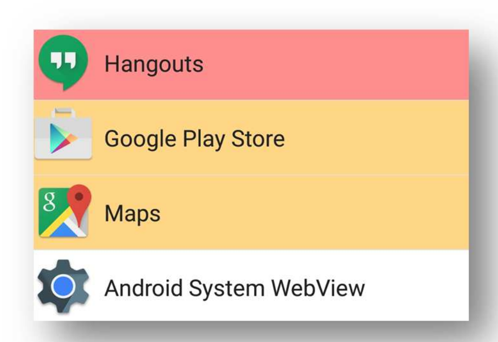




Die gesamte Blockierfunktion von SMS hat in unserem Test auf dem Nexus 5 Testgerät nicht funktioniert, da es Limitierungen von Android mit Versionen größer 4.4 gibt. Auf dies wurde von Sophos auch entsprechend hingewiesen. Die Blockierfunktion von Telefonanrufen hat wie erwartet funktioniert.

Privacy Advisor

Der Privacy Advisor listet jene installierten Apps, die für den Nutzer eine Bedrohung bezüglich der Verletzung der Privatsphäre darstellen können. Sophos kategorisiert die Apps nach Bedrohungsstufe (hoch, mittel, niedrig) und färbt die Apps in der Liste mit rot, gelb und weiß ein.



Der Nutzer hat die Möglichkeit nach folgenden Bedrohungsarten zu filtern: Verursachung von Kosten, Zugriff auf persönliche Informationen, Internetzugriff. Durch Antippen einer Applikation werden die Berechtigungen sehr detailliert beschrieben.

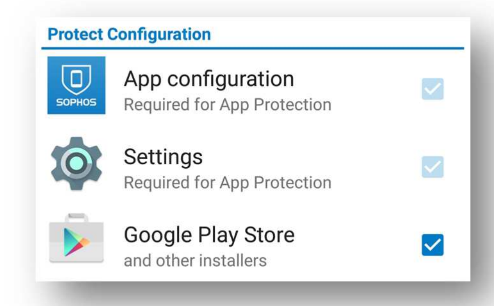
Security Advisor

Der Security Advisor macht den Nutzer auf Einstellungen auf dem Telefon aufmerksam, die die Sicherheit beeinträchtigen könnten. Sophos überprüft sieben Einstellungen etwa ob eine Bildschirmsperre oder eine Geräteverschlüsselung aktiviert ist. Durch Klicken auf einen der Einträge wird der Nutzer zu einer Erklärung und einem Button, der direkt zur entsprechenden Einstellung in den Android Settings führt, geleitet.

App Protection

Diese Komponente ermöglicht das Schützen von installierten Apps mit einem mindestens vierstelligen Passwort. Hierfür wird das Programm als Geräteadministrator eingerichtet. Anschließend erscheint eine Warnung, dass sich die App Protection mithilfe von Taskmanagern umgehen lässt. Hierfür bietet Sophos Abhilfe durch ein weiteres App, Sophos Security & Antivirus Guard, das sicherstellt, dass die Sicherheitssuite nie beendet wird.

Der einstellbare Parameter *Grace Period* definiert jene Zeit, für die die App nach dem Entsperren ohne weitere Passworteingabe zugänglich bleibt, bevor sie wieder gesperrt wird. Als Selbstschutz hat Sophos sich selbst, sowie die Android Einstellungen mit einem Passwort versehen.



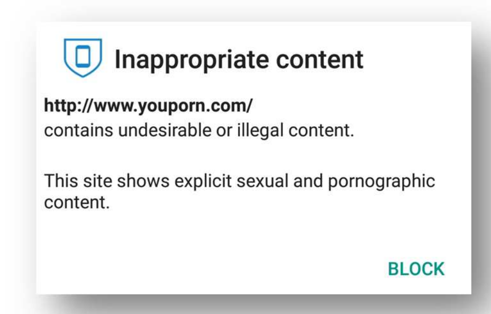
Dieser kann nicht deaktiviert werden. Aus einer Liste können weitere installierte Apps gewählt werden, welche ebenfalls mit demselben Kennwort versehen werden sollen. In unseren Tests hat diese Funktion sehr verlässlich



funktioniert und konnte nicht umgangen werden.

Web Filtering

Diese Komponente schützt den Nutzer während des Surfens im Internet vor schadhaften Webseiten. Zusätzlich kann nach Inhalten gefiltert werden, wie z.B. Alkohol, Drogen oder Waffen. All diese Kategorien sind standardmäßig auf „allow“ gesetzt. Diese Komponente lässt sich somit auch als Kindersicherung einsetzen.



In unseren Tests hat diese Komponente sehr gut und verlässlich funktioniert. Eigenartig ist, dass sich zwischen den angebotenen Kategorien auch „Phishing & Fraud“, sowie „Spyware“ findet. Auch diese sind standardmäßig auf „allow“ gesetzt. Wir finden, dass diese Kategorien in die Kategorie „Malicious Websites“ verschoben und standardmäßig zumindest auf „Warn“ oder gar „Block“ gesetzt sein sollten.

Updates

Updates werden automatisch durchgeführt, können aber auch manuell angestoßen werden. In den Einstellungen kann definiert werden ob Updates im Mobilfunknetz, bei Roaming oder nur bei WiFi Verbindung durchgeführt werden sollen.

Hilfe

Es existiert eine Hilfedatei, welche zu allen Funktionen umfangreiche Hilfestellungen bietet.

Deinstallation

Sofern die App Protection aktiviert ist wird ein Kennwort für die Deinstallation benötigt. Anschließend lässt sich das App über die Android App Verwaltung deinstallieren.

Lizenz

Sophos Mobile Security ist gratis und kann über den Google Play Store installiert werden.

Fazit

Mit Sophos Mobile Security erhält der Nutzer eine umfangreiche und gut umgesetzte Sicherheitsapp die in unserem Test durchaus überzeugen konnte. Wie auch andere Produkte hatte Sophos Probleme mit dem Blocken von SMS Nachrichten sowie mit der Sperrung mittels des nativen Android Sperrbildschirmes was auf die aktuelle Android Version zurückzuführen ist.



Tencent Mobile Manager

Tencent Mobile Manager ist eine gratis erhältliche App mit vielen verschiedenen Funktionen rund um Malware- und Datenschutz. Tencent hat dem Produkt erneut verändert und die Benutzbarkeit der App verbessert.



Installation

Die Installationsdatei wurde aus dem chinesischen App Store *„HIAPK“* heruntergeladen und installiert. Beim ersten Start muss den Nutzungsbedingungen zugestimmt werden, welche bereits als akzeptiert markiert sind.

Nach dem Start wird ein erster Systemcheck durchgeführt. Das Resultat bewertet die aktuelle Sicherheit des Gerätes. Es wird uns angeboten das Gerät per *„One click tuning“* zu optimieren. Bei dessen Ausführung werden wir darauf hingewiesen, dass die „Zahlungsumgebung“ und der „QQ instant Messenger“ nicht geschützt sind. Das Tuning beendet Prozesse, befreit Speicher, leert den App Cache, führt einen Virenscann durch und überprüft ob der Web Blocker aktiviert ist. Die App schlägt uns außerdem vor, die *„Secure SMS“* Komponente als Standard SMS-Dienst zu verwenden.

Das Hauptmenü zeigt die Optionen *„Clean up & Speed-up“*, „Security“, *“App Management”* und *“Expert-Tools”*.

Clean up & Speed-up



In diesem Menüpunkt bietet Tencent vier Bereinigungsfunktionen an. Es handelt sich um einen Mobile-Speed-Up, Junk Removal, einen Speicher Manager sowie die Möglichkeit den Startvorgang von Apps beim Start zu beeinflussen.

Security

Unter diesem Menüpunkt sind neben dem Virenscan die Funktionen Datenüberwachung, Spam Call Blocker, Werbeblocker und ein Schutz gegen ungewünschte Zahlungen zu finden.





Data Traffic Monitor

Mit dem „Data Traffic Monitor“ kann der tägliche und monatliche Datenverbrauch angezeigt werden. Die aufgezeichneten Resultate können mit den Aufzeichnungen des Mobilfunkanbieters synchronisiert werden um die Nutzung des gekauften Datenpaketes besser überwachen zu können.

Spam Call Blocker

In unseren Tests konnte der Spam Call Blocker chinesische Spam SMS und Anrufe von ungewollten Nummern blocken.

Ad blocker

Der Werbeblocker blockt Werbeeinblendungen in Apps - diese Komponente funktioniert allerding nur auf einem gerooteten Handy.

Payment Protection

Diese Komponente stellt eine sichere Umgebung, für Apps wie Alipay Wallet oder WeChat zur Verfügung. Der Nutzer kann solche Apps direkt von dieser Komponente aus starten. Bevor eine App gestartet wird überprüft die *„payment protection“* gefälschte QR Codes, Phishing, gefälschte WLAN-Zugänge und gefälschte Zahlungsapps.

Alle, für Zahlungsapps relevante, Kurznachrichten können direkt in der App betrachtet werden.

Zusätzlich wird noch eine weiterer „geschützter Bereich“ angeboten, von welchem verschiedene Chinesische Onlinebankingapps heruntergeladen und gestartet werden können.



AV Scan

Als Neuerung zum Vorjahr zeigt diese Komponente nun auch Apps an welche Werbung enthalten. Der Nutzer kann in die Werbeblocker Komponente wechseln oder potentielle Malware melden.

In den AV Scan Settings kann der „Smart Scan“, „Quick Scan“ oder „Full Scan“ als Scanmethode gesetzt werden. Zusätzlich kann eine zusätzliche „Trojaner-Entferner“ Komponente installiert werden, welche das Gerät auf sieben verschiedene Trojaner Typen untersucht.

App Management

Hier listet Tencent verschiedene empfohlene Apps und bietet die Verwaltung von bereits installierten Apps, die Deinstallation sowie die Rechteverwaltung von Apps an. Für die Rechteverwaltung ist wiederum Rootzugriff notwendig.



Expert Tools

Diese Komponente bietet zusätzliche Tools wie etwa dem „Privacy Space“, App Lock, Anti-Theft Protection, ein Tool um offene WLAN-Spots zu erkennen und mit ihnen zu verbinden sowie einen sicheren QR-Code Scanner. Zusätzlich ist es in dieser Komponente möglich vorgeschlagene Spiele und andere Tools von Tencent wie z.B. „WeSync“, „QQ Browser“ und den „QQ App Store“ zu installieren.

Auf einer weiteren Seite befinden sich noch ein Batterie Manager in Form einer weiteren App und die Möglichkeit sein mobiles Guthaben aufzuladen. Außerdem ein Tool um den Netzanbieter und zusätzliche Informationen zu einer Telefonnummer zu erhalten.

Privacy Space

Um dieses Tool zu verwenden muss zuerst ein Passwort gesetzt werden. Dann kann es benutzt werden um Fotos, Videos, SMS von bestimmten Telefonnummern und Dateien zu verstecken. Fügt man etwa Fotos zum Privacy Space hinzu scheinen diese nur noch hier nicht mehr aber in der normalen Fotogalerie auf.

Anti-Theft

Die Anti-Theft Komponente funktioniert nur in Verbindung mit dem Tencent Instant Messenger QQ. Nach der Aktivierung ist die QQ Nummer das standardmäßige Passwort um auf die Anti-Theft Komponente zuzugreifen. Sie kann über ein Webinterface kontrolliert (m.qq.com) werden. Zusätzlich kann mit der „Help others to locate their mobile phone“ Funktion jedes Telefon, auf dem QQ Mobile Manager installiert ist, gefunden werden.

Es ist möglich das Gerät zu lokalisieren, zu sperren, persönliche Daten zu löschen und einen Alarm abzuspielen. Um sich vor der Deinstallation zu schützen muss die App als Geräte Administrator eingetragen werden.

Über „Freeze QQ/WeChat“ erhält der User Informationen um unautorisierte Zugriffe auf seinen „QQ“ oder „WeChat“ Account zu melden.

Updates

Virendefinitionen werden automatisch durchgeführt. Zudem können manuell Aktualisierungen angestoßen werden.

Lizenz

Tencent Mobile Manager ist kostenlos verfügbar.

Hilfe

Tencent Funktionen sind in der App oder auf einer dazugehörigen Webseite erklärt.

Deinstallation

Für die Deinstallation wird kein Password benötigt.

Fazit

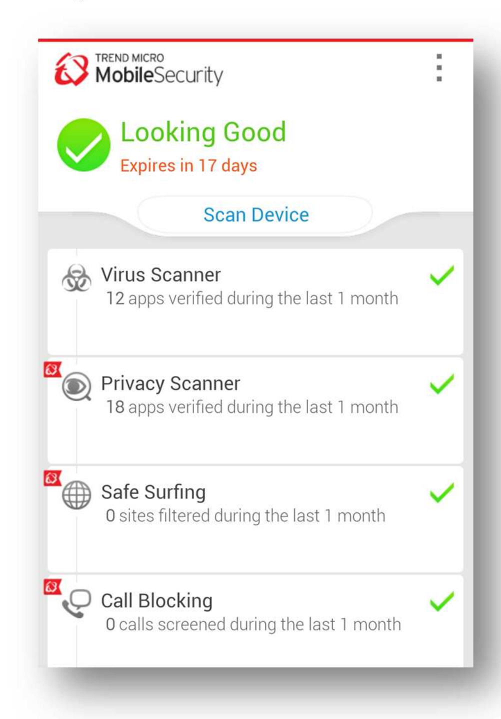
Die Anti-Theft Funktion kann nun nur noch in Verbindung mit einem „Tencent QQ Messenger“ Account benutzt werden. Gefallen hat uns, dass die „WeChat Protection“ in das Anti-Theft Menü eingebunden ist. Auf unserem Testgerät haben alle Anti-Theft Funktionen funktioniert. Beim „Wipe“ wurde allerdings auf das Ausloggen der Accounts (Google, QQ, WeChat) vergessen.

Natürlich steht es jedem Hersteller frei weitere Standalone-Apps zur Installation zu empfehlen. In unseren Augen gilt dies nur für Apps mit echtem Mehrwert. Tencent sollte darauf achten es nicht mit derartigen Empfehlungen zu übertreiben. Außerdem sehen wir die Empfehlung das Gerät zu rooten als sehr kritisch.



Trend Micro Mobile Security

Trend Micro Mobile Security ist eine kostenpflichtige aber umfangreiche Sicherheits-App. Neben dem obligatorischen Virus Scanner und der Anti-Theft Komponente bietet sie z.B. noch eine Safe Surfing & Parental Control Komponente die aktiven Schutz beim Surfen im Internet bietet. Neu in der aktuellen Version ist sogenannte „System Tuner“ mit dessen Hilfe etwa die Akkulaufzeit verlängert werden kann.



Installation

Trend Micro Mobile Security wurde aus dem Google Play Store bezogen und installiert. Nach dem Akzeptieren der EULA wird eine kurze Einführung gegeben, bevor der Nutzer auf den Startbildschirm weitergeleitet wird.

Virus Scanner

Durch Klick auf den Button für den Virus Scanner wird der Nutzer entsprechend weitergeleitet. Dort findet sich ein Button zum sofortigen Scannen des Geräts, sowie einer Vielzahl von Einstellmöglichkeiten, unter anderem ob die die SD Karte gescannt, oder der Echtzeitscanner aktiviert werden soll.

Privacy Scanner

Der Privacy Scanner überprüft die auf dem Gerät installierten Apps auf mögliche Risiken bezüglich der Spionage von privaten Daten oder aggressiven Werbungen. Trend Micro bietet für diese Komponente auch einen Echtzeitscanner, der bei der Installation von neuen Programmen sofort eine derartige Überprüfung vornimmt. Mögliche Bedrohungen werden in Gefahrenkategorien eingeteilt. In unseren Tests wurden „Low“ und „Medium“ Risks angezeigt. Durch Antippen eines Eintrags werden Details zu den jeweiligen Berechtigungen, sowie eine kurze Erklärung angezeigt. Anschließend kann die Applikation entweder deinstalliert oder einer Liste von vertrauenswürdigen Apps hinzugefügt werden.

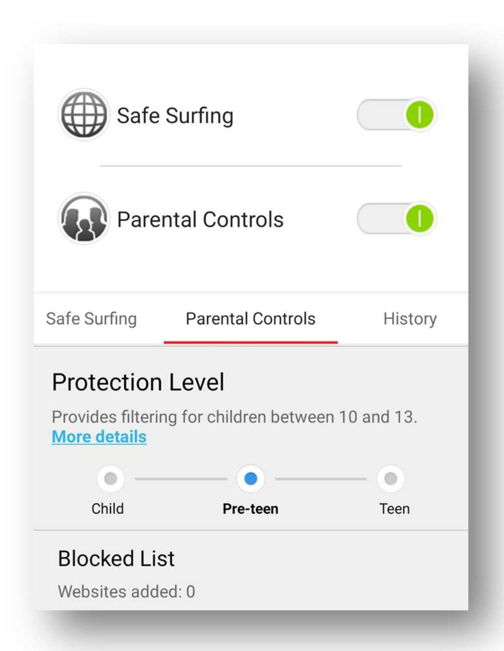
Safe Surfing & Parental Control

Unter dieser Komponente fasst Trend Micro Schutzfunktionen bezüglich des Surfens im Internet, sowie Kindersicherung, zusammen.

Das Safe Surfing schützt den Nutzer beim Browsen im Internet. Dabei kann als Sicherheitsstufe hoch, mittel oder niedrig eingestellt werden. Während bei „hoch“ Webseiten mit jedem geringsten Risiko geblockt werden, ist Trend Micro mit der Einstellung „niedrig“ ein wenig nachsichtiger und ignoriert weniger gefährliche Bedrohungen.

Für Parental Control muss erst das Kennwort des Trend Micro Accounts eingegeben werden. Danach kann ein Schutz speziell für den internetsurfenden Nachwuchs eingestellt werden. Hierbei hat der Nutzer die Möglichkeit den Schutz speziell auf das Alter abzustimmen (Child, Pre-Teen und Teen). Zusätzlich zur Voreinstellung können Webseiten auf eine Black- oder Whitelist gesetzt werden.



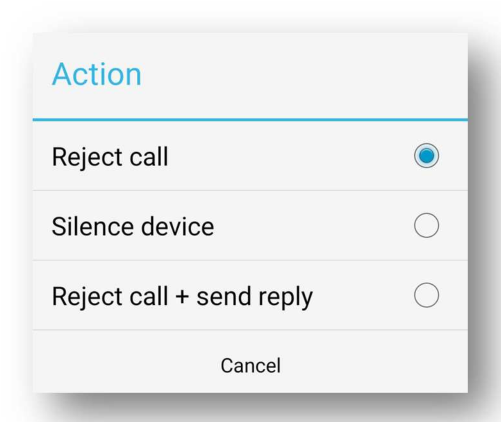


Mit der Uninstall-Protection kann verhindert werden, dass das Kind oder der Jugendliche die App einfach deinstalliert. Diese Funktion würden wir nicht nur dem Jugendschutz zuordnen, sondern z.B. auch dem Diebstahlschutz. Deshalb würden wir einen globalen Deinstallationsschutz für sinnvoller halten. Der Deinstallationsschutz war allgemein sehr verlässlich und konnte in unseren Tests nicht umgangen werden. In einem Verlauf können geblockte Webseiten angezeigt werden. Dies trifft sowohl für gefährliche Homepages, als auch für solche die aufgrund des Jugendschutzes blockiert wurden, zu.

In unserem Test konnten wir trotz aktiviertem Parental Control Feature zu einem Gastkonto wechseln. Dort konnten sämtliche geblockte URLs angesurft werden. Auf diesen Zustand sollte Trend Micro hinweisen.

Call Blocking

Call Blocking bietet das Blockieren von unerwünschten Anrufen. Hierfür kann entweder Blacklisting oder Whitelisting gewählt werden. Während dem Whitelisting kann noch die Option aktiviert werden, dass Anrufer mit unterdrückter Nummer akzeptiert werden.



Zusätzlich lässt sich die Aktion einstellen, welche bei einer erfolgreichen Sperrung ausgeführt werden soll. Hierfür stehen dem Nutzer die Möglichkeiten „Abweisen“, „Gerät stumm stellen“ und „Abweisen + SMS Antwort senden“ zur Verfügung. Für die SMS Antwort kann entweder einer der drei vordefinierten Texte, oder ein manuell eingegebener gewählt werden.

Lost Device Protection

Unter Lost Device Protection versteht Trend Micro den Diebstahlschutz. Es werden die klassischen Schutzfunktionen wie Lokalisieren, Sperren und Löschen angeboten. Gesteuert werden die Kommandos über ein Webinterface. SMS Kommandos existieren nicht.

Zum Ändern jeglicher Einstellungen betreffend der Lost Device Protection ist ein Passwort erforderlich, damit ein Dieb nicht einfach die Diebstahlsicherung deaktivieren kann.

Locate

Die Locate Funktion lokalisiert das Gerät und zeigt die Position in einer Google Maps Karte an. Die Aktion wird automatisch ausgeführt, wenn das Webinterface geöffnet wird. Die Position kann auf Facebook geteilt werden.

SIM Card Lock

Der SIM Card Lock sperrt das Gerät, wenn die SIM Karte entweder entnommen oder eine andere eingelegt wird. Der SIM Lock hat in unserem Test etwas lange gedauert. Ein Dieb hat somit die Möglichkeit nach einem Neustart des Geräts es für rund 10 Sekunden



uneingeschränkt zu verwenden. Durch diese Verzögerung war es uns möglich nach mehreren Versuchen die App zu deinstallieren bevor der Lockscreen das Gerät sperrte. Um dieses Problem zu beheben rät Trend Micro dazu die „Uninstall Protection", die sich in der „Safe Surfing & Parental Control" Komponente befindet, zu aktivieren.

Lock

Mit dieser Funktion wird das Gerät gesperrt und somit der Zugriff für Dritte unmöglich gemacht. Es kann nur mit einem gültigen Passwort wieder entsperrt werden. Es besteht die Möglichkeit ein neues Passwort via E-Mail zu versenden. Ein Notruf Button wurde integriert, in unserem Test wurde der Notrufbildschirm allerdings sofort wieder vom Lockscreen verdeckt.

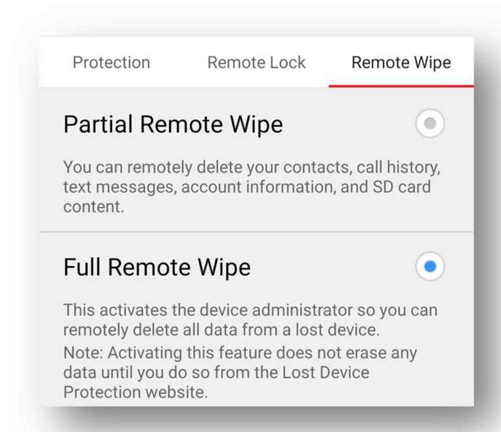
Wir konnten weder die Notification Leiste öffnen, noch den Sperrbildschirm auf herkömmliche Weise umgehen. Auch hier tritt das oben genannte Problem mit der Verzögerung des Lockscreens auf. Demnach wäre es möglich das Gerät so lange uneingeschränkt zu verwenden um die App zu installieren.

Sirene

Dieser Befehl lässt einen Alarm ertönen. Dabei wird das Gerät nicht gesperrt, es dient also nur dem Wiederfinden innerhalb der eigenen vier Wände.

Wipe

Beim Wipe bietet Trend Micro zwei Varianten an: Den Partial Remote Wipe, der persönliche Daten vom Gerät löscht, und einen Full Remote Wipe, der zusätzlich das Gerät auf Werkseinstellungen zurücksetzt.



Der Wipe hat im Großen und Ganzen gut funktioniert, jedoch wurde bei der Verwendung des "Partial Wipes" der Browserverlauf und die Favoriten nicht gelöscht. Wie zu erwarten konnte auch Trend Micro die SMS auf der aktuellen Android Version nicht löschen.

Backup & Restore

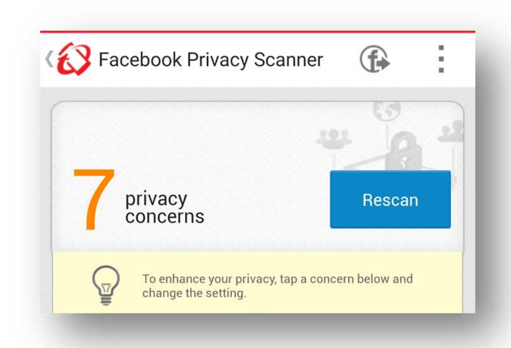
Diese Funktion ist als externe App verfügbar und ermöglicht die Sicherung von Kontakten, Kalendereinträgen, Anruf Verlauf, Text Verlauf, Fotos, Musik und Videos. Hierfür bietet Trend Micro 50MB Speicher.

Das Backup kann auch automatisch gestartet werden. Hierfür können die Wochentage eingestellt werden. Außerdem besteht die Möglichkeit das automatische Backup für Roaming und mobile Datenverbindung zu deaktivieren. Auch die Rücksicherung gestaltet sich komfortabel. Trend Micro prüft alle Änderungen auf dem Server und schlägt anschließend vor, welche Einträge zurückgesichert werden könnten.

Scan Facebook

Diese Komponente prüft das Facebookprofil des Nutzers auf datenschutzrechtlich bedenkliche Einstellungen. Dazu muss der Nutzer den Usernamen und das Passwort seines Facebook Accounts angeben. Anschließend werden alle „Privacy Concerns" aufgelistet, zum Beispiel ob andere Nutzer mit der Telefonnummer nach dem Account suchen können dürfen. Sollte der Nutzer eine Einstellung ändern wollen, so kann er dies direkt aus dem Menü tun.

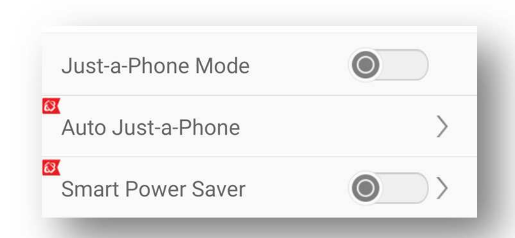




Trend Micro ändert selbstständig die entsprechenden Einstellungen in Facebook.

System Tuner

Eine neue Funktion im Vergleich zur Vorjahresversion von Trend Micro ist der System Tuner. Er bietet Optimierungen betreffend der Batterielaufzeit und der Speicherauslastung. Für erstgenannte ist es möglich das Gerät in einen „Just-a-Phone“ Modus zu versetzen, wo alle anderen Arten der Kommunikation (WiFi, Bluetooth, 3G/4G etc.) deaktiviert werden.



Gefallen hat uns, dass sich dieser Modus auch automatisch zu gewissen Zeitpunkten oder Events aktivieren lässt. Zusätzlich ermöglicht der System Tuner die Löschung des Verlaufs des Webbrowsers, der Google Play Store Suche und der Clipboard Daten.

Updates

Updates werden automatisch heruntergeladen (täglich, wöchentlich, monatlich). Es ist einstellbar, dass hierfür nur die WiFi Verbindung verwendet werden soll. Außerdem ist es möglich nach jedem Update automatisch einen Scan zu starten.

Hilfe

Trend Micro bietet eine umfangreiche Onlinehilfe an.

Deinstallation

Für die Deinstallation ist kein Passwort notwendig, es sei denn der Nutzer hat die Kindersicherung aktiviert. In diesem Fall ist eine Passworteingabe erforderlich, welche wir nicht umgehen konnten. Trend Micro hat unseren Vorschlag, den Deinstallationsschutz global verfügbar zu machen, angenommen und wird diese Funktion in folgenden Releases einbauen.

Lizenz

Trend Micro Mobile Security kann aus dem Play Store installiert werden und ist dann 30 Tage lang gratis getestet werden. Danach kann ein oder zwei Jahres Abo für € 19,95 bzw. € 29,95 erworben werden.

Fazit

Mit Trend Micro Mobile Security erhält der Nutzer ein durchdachtes Produkt bei dem es auch hier versionsbedingt bei einigen Funktionen zu Problemen kommt. Im speziellen Fall war es uns möglich den Sperrbildschirm der App komplett zu umgehen.



Permissions in Android OS 5.1.1		AhnLab	Antiy	Avast	AVG	Avira	Cheetah C.M.	Cheetah CM S.	Baidu	Bitdefender	ESET	GData	Kaspersky Lab	McAfee	Sophos	Tencent	Trend Micro
Phone calls	directly call phone numbers							•		•				•			
	read phone status and identity						•	•						•			
	reroute outgoing calls	•	•		•			•		•			•	•	•		•
Your messages	edit your text messages (SMS or MMS)							•		•				•			
	read your text messages (SMS or MMS)		•					•		•				•			
	receive text messages (SMS)		•					•		•				•			
	receive text messages (MMS)	•	•		•	•				•		•	•	•			
	receive text messages (WAP)	•	•	•	•	•		•		•	•	•	•		•		•
	send SMS messages		•					•		•				•			
Camera	take pictures and videos		•	•			•	•		•				•	•		•
Microphone	record audio	•	•	•	•	•				•	•	•	•		•	•	•
Your location	approximate location (network-based)		•	•				•		•	•			•			
	precise location (GPS and network-based)		•	•				•		•				•			
Your social information	modify your contacts		•					•		•				•			
	read call log		•					•		•				•			
	read your contacts		•					•		•				•			
	write call log		•					•		•				•			
Your personal information	activity recognition	•	•	•	•	•		•	•	•		•	•		•	•	•
	add or modify calendar events and send email to guests without owners´ knowledge		•	•		•			•	•		•	•		•	•	•
	read calendar events plus confidential information	•	•	•	•	•			•	•		•	•		•	•	•
	modify your own contact card	•	•	•	•	•			•	•		•	•		•	•	•
	read your own contact card	•	•	•	•	•			•	•		•	•		•	•	•
Bookmarks and History	write web bookmarks and history			•			•	•		•		•	•	•	•		
	read your Web bookmarks and history						•	•		•		•	•	•	•		
Storage	modify or delete the contents of your USB storage						•	•						•			•
	read the contents of your USB storage						•	•						•		•	•
Alarm	set an alarm	•	•	•	•	•	•		•	•	•	•	•		•	•	•
Lock screen	disable your screen lock	•	•	•						•		•	•	•	•		•
Your accounts	add or remove accounts		•	•				•	•	•			•		•	•	
	find accounts on the device		•				•	•		•			•	•	•		
	read Google service configuration	•	•		•			•	•	•	•		•		•	•	•
	use accounts on the device		•		•			•	•	•	•	•	•	•	•	•	
	create accounts and set passwords	•	•	•	•	•			•	•	•		•		•	•	•
Read user dictionary	read terms you added to the dictionary	•	•	•	•	•			•	•	•	•	•		•	•	•
Network communication	change network connectivity	•	•	•	•	•	•	•		•		•		•	•		
	connect and disconnect from Wi-Fi	•	•			•	•	•		•				•	•		
	download files without notification							•									
	control Near Field Communication	•	•		•	•			•	•	•	•	•			•	•
	Google Play billing service		•	•					•	•				•	•	•	
	Google Play license check	•	•	•	•	•			•	•	•		•	•	•	•	•
	receive data from Internet	•	•				•	•	•	•				•	•	•	
	full network access						•	•						•			
	view network connections						•	•						•			
	view Wi-Fi connections		•				•	•						•			
Bluetooth	access Bluetooth settings	•	•	•		•		•		•	•		•	•	•		
	pair with Bluetooth devices	•	•	•		•		•		•	•		•	•	•		
Your application information	close other apps		•			•	•	•		•	•	•		•			
	reorder running apps	•	•	•	•	•				•	•		•	•	•		•
	retrieve running apps						•	•		•				•			
	run at startup		•					•						•			
Other Application UI	draw over other apps			•			•	•		•		•		•	•		
Affects Battery	allow Wi-Fi Multicast reception	•	•	•	•	•				•	•	•	•		•		•
	control flashlight	•	•	•	•	•				•	•	•	•		•		•
	control vibration		•			•	•	•			•			•	•		
	prevent phone from sleeping						•	•		•				•			
Wallpaper	adjust your wallpaper size	•	•	•	•	•				•	•	•	•		•	•	•
	set wallpaper	•	•	•	•	•				•	•	•	•		•	•	•
Write user dictionary	add words to user-defined dictionary	•	•	•		•			•	•	•	•	•		•	•	•
Audio Settings	change your audio settings	•	•	•			•	•		•	•	•			•	•	
Sync Settings	read sync settings	•	•	•		•				•	•	•		•	•	•	
	read sync statistics	•	•	•	•	•				•	•	•	•	•	•	•	•
	toggle sync on and off	•	•	•		•				•	•	•		•	•		
Status Bar	expand/collapse status bar	•	•	•	•		•			•	•	•			•	•	•
System tools	access extra location provider commands	•	•	•	•	•			•	•	•	•			•		•
	delete all app cache data		•	•		•	•	•		•		•	•		•		•
	install shortcuts	•	•	•		•	•	•		•	•	•	•		•		•
	measure app storage space	•	•			•	•	•		•	•		•	•	•		
	mock location provider commands	•	•	•	•	•			•	•	•	•	•		•	•	•
	mock location sources for testing	•	•	•	•	•			•	•	•	•	•		•	•	
	modify system settings	•	•			•	•	•		•	•			•	•		
	read Home settings and shortcuts	•	•	•	•	•			•	•	•	•			•	•	•
	read subscribed feeds	•	•	•	•	•			•	•	•	•	•		•	•	•
	send sticky broadcast	•	•	•	•	•	•			•	•		•		•		•
	uninstall shortcuts	•	•	•		•	•	•		•	•	•	•		•		•
	write Home settings and shortcuts	•	•	•		•			•	•	•	•	•		•	•	•

Feature List Android Mobile Security (as of August 2015)	*FREE*	FREE	FREE	COMMERCIAL	FREE	COMMERCIAL	FREE	COMMERCIAL	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	FREE	FREE	COMMERCIAL
Product Name	*Android OS*	AhnLab V3 Mobile Security	Antiy AVL for Android	Avast Mobile Security & Antivirus	Avira Antivirus Security	AVG AntiVirus	Baidu Mobile Guard	Bitdefender Mobile Security & Antivirus	Cheetah Mobile Clean Master	Cheetah Mobile CM Security Antivirus	ESET Mobile Security & Antivirus	G Data Internet Security	Kaspersky Internet Security	McAfee Security & Antivirus	Sophos Free Antivirus and Security	Tencent Mobile Manager	Trend Micro Mobile Security & Antivirus
Version Number	*5.1.1*	3.0.3.4	2.3.12	4.0.7886	4.1	4.4	6.6.0	3.0.135	2.6.8	5.10.3	3.0.1318	25.8.3	11.8.4.625	4.4.0.467	5.0.1515	5.6.0	6.0
Supported Android versions	*built-in*	2.2 and higher	2.1 and higher	2.2 and higher	2.2 and higher	2.2 and higher	2.2 and higher	2.3.3 and higher	2.2 and higher	2.2 and higher	2.3 and higher	2.1 and higher	2.3 and higher	2.3 and higher	2.3.3 and higher	2.1 and higher	2.3 and higher
Supported Program languages	All	English, Korean	English	English, Czech, French, Italian, Spanish, German, Russian, Portuguese, Catalan, Hungarian, Dutch, Polish, Turkish, Vietnamese, Chinese, Japanese, Bulgarian	English, German, French, Italian, Spanish, Korean, Japanese, Portuguese	English	Chinese	English, Portuguese, French, German, Italian, Polish, Romanian, Spanish, Turkish, Vietnamese	Chinese	English, Russian, Spanish, Italian, Indonesian, Turkish, German, Portuguese, French, Vietnamese, Arabic, Thai, Japanese, Korean, Hungary, Croatian, Greek, Malay, Dutch, Slovak, Bulgarian, Ukrainian, Polish, Serbian, Chinese	English, Polish, Danish, Finnish, Norwegian, Japanese, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Swedish, Chinese, Italian, French, Korean, Czech, Hebrew, Slovak, Vietnamese, Arabic, Bulgarian, Thai	German, English, French, Spanish, Portuguese, Italian, Dutch, Polish, Russian, Turkish, Japanese, Chinese	English, Russian, German, French, Spanish, Italian, Portuguese	English, Danish, German, Greek, Spanish, Finnish, French, Indonesian, Italian, Japanese, Korean, Norwegian, Dutch, Portuguese, Russian, Swedish, Turkish, Chinese	English, German, French, Italian, Japanese, Chinese	Chinese	English, German, Spanish, French, Italian, Korean, Dutch, Portuguese, Chinese, Turkish, Vietnamese
Anti-Malware																	
On-Install scan of Installed apps	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-Demand scan		●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
On-Access scan for files			●	●					●		●	●	●	●	●	●	
Scan works offline		●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
Scan is assisted by cloud	●			●	●	●		●	●	●	●	●	●	●	●	●	●
Automatic (scheduled) Scan		●	●	●		●				●	●	●	●	●	●	●	●
Safe Browsing (Anti-Phishing & Anti-Malware)	●		●	●		●		●	●	●	●	●	●	●	●	●	●
Scan installed apps for (possible) privacy violations	●		●	●		●	●	●		●	●	●		●	●	●	●
Quarantine										●	●		●		●		
Recommendations for android settings	●						●				●			●	●	●	
USSD Blocking	●			●	●						●	●	●	●	●		
Anti-Theft																	
Remote Lock & Remote Wipe	●	●		●	●	●		●		●	●	●	●	●	●	●	●
Remote Locate	●	●		●	●	●		●		●	●	●	●	●	●	●	●
Remote Alarm	●			●	●	●		●		●	●	●	●	●	●	●	●
SMS commands for controlling Anti-Theft features		●		●		●		●		●	●	●	●	●	●	●	
Webinterface for controlling Anti-Theft features	●			●	●	●		●		●	●		●	●		●	●
Notify on SIM Change (Email / SMS)		●		●		●		●		●	●	●	●	●	●	●	
Lock on SIM Change		●		●		●				●	●	●	●	●		●	●
Remote Unlock				●	●	●				●	●			●	●	●	
Anti Spam																	
Whitelist / Blacklist Phonecalls		●		●	●	●	●			●	●	●	●	●	●	●	●
Whitelist / Blacklist SMS		●		●	●		●				●	●	●	●	●	●	●
Whitelist / Blacklist with wildcards				●			●				●	●	●	●	●	●	
Blocking of SMS containing keywords		●					●						●	●		●	●
Parental Control																	
Safe Webbrowsing				●				●		●		●		●	●		●
Lock Apps				●		●		●		●		●		●	●	●	
App launcher especially for kids (Parents can choose apps)												●		●			
Authentication																	
Uninstallation protection (password required for uninstallation)				●		●		●			●	●	●	●	●	●	●
Settings protected with password				●		●					●	●	●		●	●	●
User Account needed to use product	●				●			●				●	●				●
Additional features																	
Backup	●			●		●						●		●		●	●
Network monitor		●		●		●	●				●			●		●	
Local Wipe	●			●		●	●	●					●	●			
Task Killer	●			●		●	●		●					●		●	
Battery Monitor	●					●					●			●			
Support																	
Online Help	●	●		●	●	●		●	●	●	●	●	●	●	●	●	●
FAQ	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●
Email support		●	●	●	●	●		●	●	●	●	●	●	●		●	●
User Forum	●			●	●	●		●	●	●	●		●	●	●	●	●
User Manual	●	●		●	●		●	●			●	●	●	●		●	
Phone Support				●	●	●		●	●		●	●	●	●		●	●
Online Chat								●	●				●	●		●	
Supported languages of support	All	English, Korean	English, Chinese	English, Czech, French, Spanish, Portuguese, Turkish, Polish, Russian, German, Chinese, Italian	German, English, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malaysian, Korean	English, German, Czech, French, Italian, Dutch, Polish, Spanish, Portuguese	Chinese	English, French, Italian, Spanish, Portuguese, Romanian, German, Turkish	Chinese	Chinese	All	German, English, Spanish, Italian, French, Portugese, Chinese, Japanese	English, Russian, German, French, Spanish, Italian, Portuguese	Spanish, English, Portuguese, Czech, Danish, German, French, Chinese, Italian, Japanese, Dutch, Norwegian, Polish, Russian, Suomi, Swedish, Turkish, Korean	English, German, French, Italian, Japanese, Chinese	Chinese	English

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives (September 2015)

